

Villarreal, Monique

From: Joseph, Paul
Sent: Tuesday, June 26, 2018 2:41 PM
To: Villarreal, Monique
Subject: Fw: Emailing: California cops 4th Largest Agency to Use Facial Recognition
Attachments: Canada police deploy fac...pdf; Face_Recognition_NeoFace_Watch_Brochure.pdf; Facial recognition Chula Vista.pdf; Facial Recognition Technology Chicago Police Policy.pdf; FBI begins installation ...pdf; Police Chief Magazine - Facial Recognition software.pdf; The top 6 FAQs about facial recognition.pdf; UK, the world's most Facial Recognition software.pdf; vorder_bruegge-Facial-Recognition-and-Identification-Initiatives FBI.pdf; California cops 4th Largest Agency to Use Facial Recognition.pdf

From: Williams, Shawny
Sent: Wednesday, October 25, 2017 10:29 AM
To: Schroder, Edward; Joseph, Paul
Cc: Tindall, David; Spagnoli, Paul
Subject: Emailing: California cops 4th Largest Agency to Use Facial Recognition

ED/PJ

I am providing you with some information about (Biometric Identification Systems) Facial Recognition technology and departments that are currently utilize it. I would like for us to complete our research and setup a presentation for the Chiefs by the beginning of December.

Your message is ready to be sent with the following file or link attachments:

California cops 4th Largest Agency to Use Facial Recognition

Note: To protect against computer viruses, e-mail programs may prevent sending or receiving certain types of file attachments. Check your e-mail security settings to determine how attachments are handled.

Canada police deploy facial recognition tech

Published time: November 07, 2014 02:31

<http://on.rt.com/9xniua>



Reuters / Tri. Gaillard

Facebook

Twitter

Reddit

StumbleUpon

Google+

Tumblr

Tags

Canada, Information

Technology, Law, Police, Security, USA

Canada is adopting some of its North American neighbor's controversial police methods and dipping its toes into the pool of facial recognition technology, with Calgary police paving the way for a full-scale automated biometric identification system.

Beginning this month, the Calgary Police Service will start taking advantage of this software to compare mugshots with videos and photographs captured from crime scenes, [CBC](#) reported on Tuesday. Instead of manually sifting through a database consisting of 300,000 mugshots, police will now be able automate that process significantly.

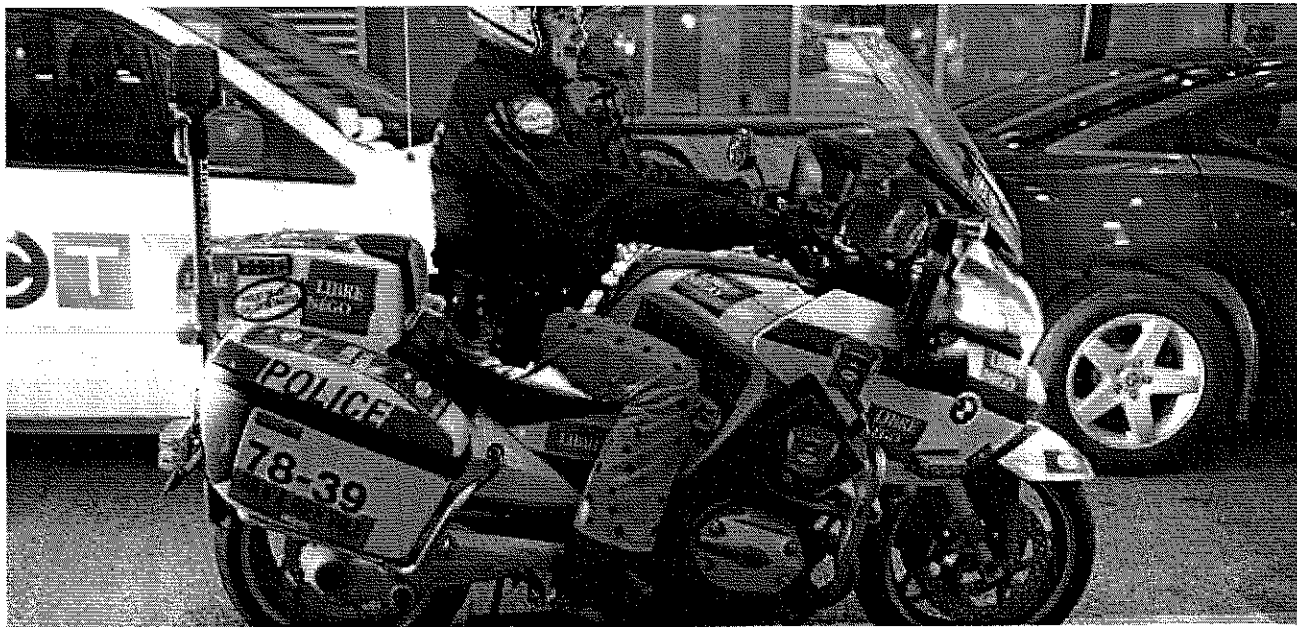
Once the department starts doing so, it will become the first law enforcement agency in Canada to employ facial recognition technology.

According to officials, the system works via a *"complex mathematical algorithm of pattern recognition to quickly screen a database of photos for potential matches."*

Quick to comfort those concerned over civil liberties or potential surveillance, Inspector Rosemary Hawkins said the software would only be used in cases where there is an open police investigation.

"This technology will not be used to identify people walking down the street as a member of the general public," she said to CBC. *"It will be used to identify subjects involved in criminal activity under police investigation and the image searched against our mugshot database, which holds photos of people that have been processed on charges."*





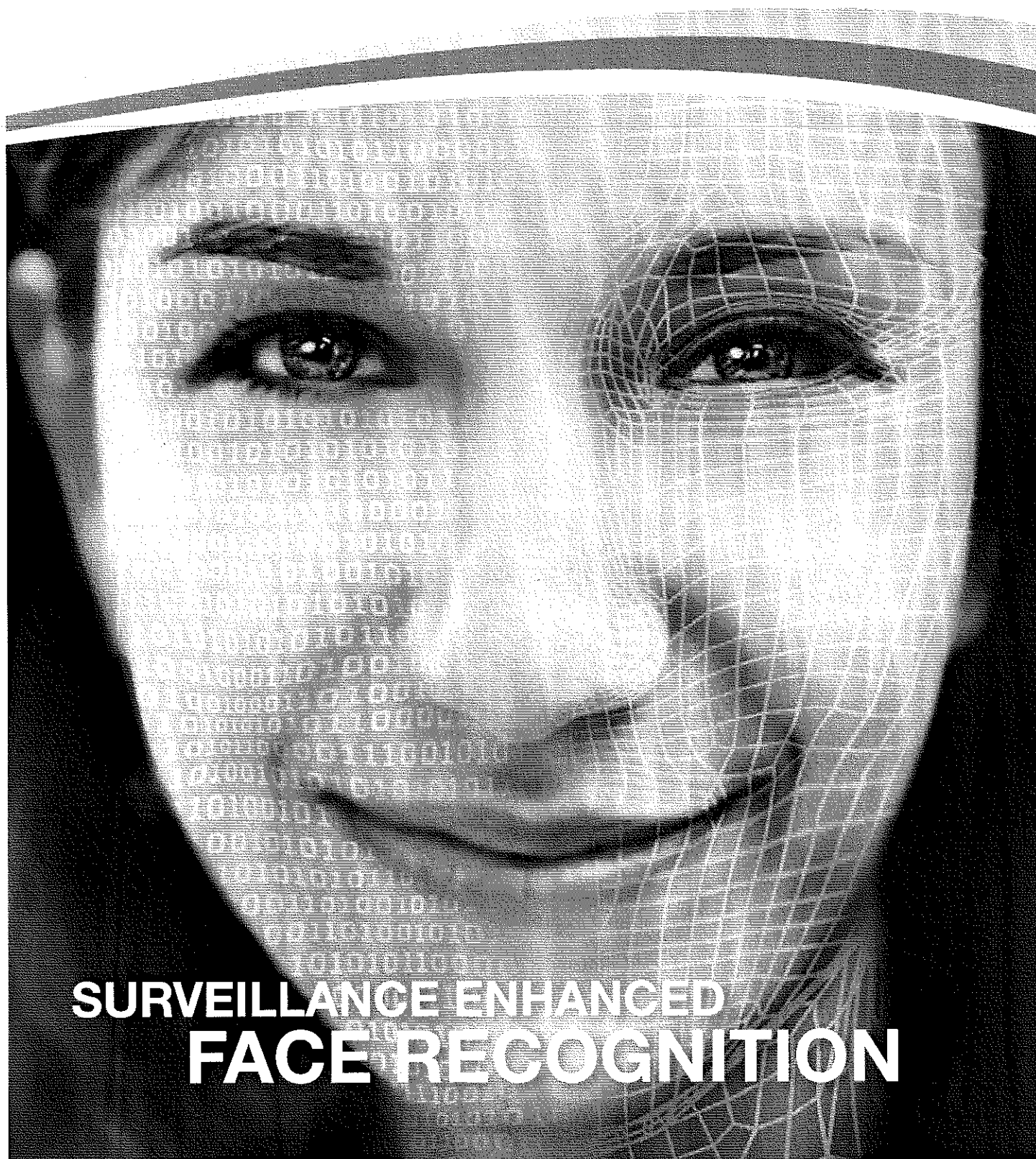
[AP Photo / Mike Locantore](#)

The news follows expanded use of facial technology by law enforcement in the United States. In September, the FBI announced its new biometric database, the Next Generation Identification System (NGI), is fully operational. Developed over the course of three years, the NGI contains over 100 million individual records – linking a person's fingerprints, palm prints, iris scans and facial-recognition data with personal information like their home address, age, legal status and other details.

Already, the FBI has used its software to successfully apprehend a man suspected of child sex abuse. He was on the run for 14 years before being detained in Nepal. By 2015, the NGI database is projected to feature 52 million facial recognition images.

Empowered by Innovation

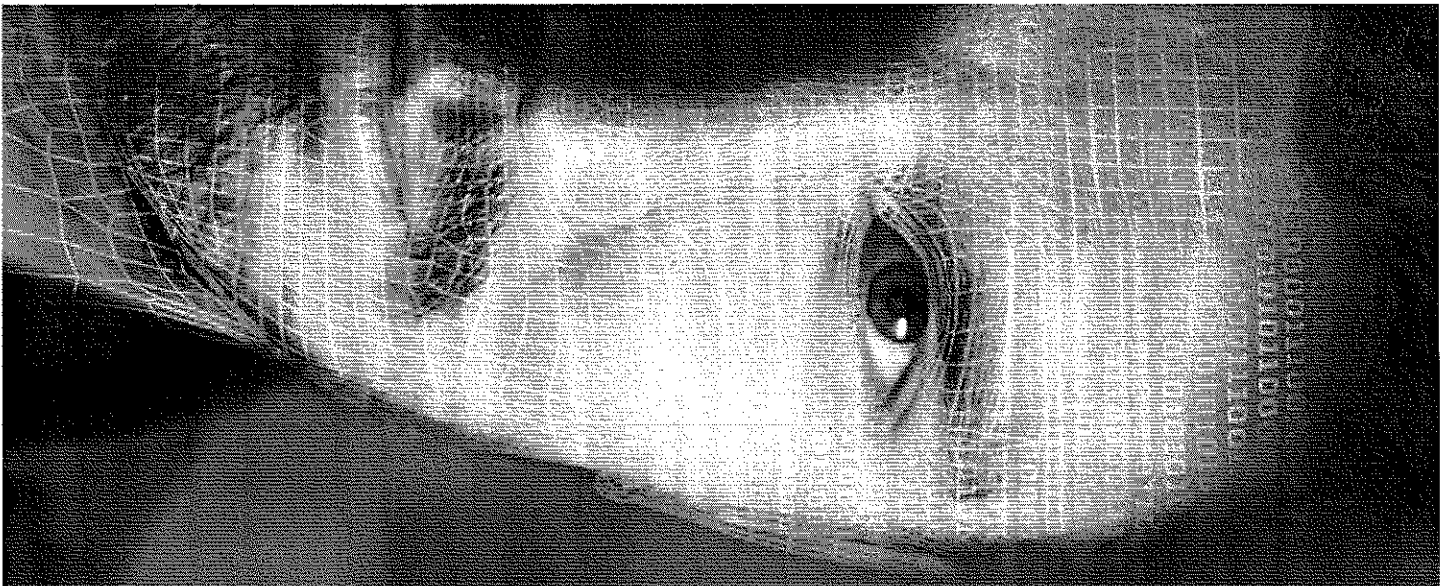
NEC



SURVEILLANCE ENHANCED FACE RECOGNITION



- ▶ Citizen Services & Immigration Control ▶ Law Enforcement
- ▶ Critical Infrastructure Management ▶ Public Administration Services
- ▶ Information Management ▶ Emergency & Disaster Management ▶ Inter-Agency Collaboration



BIOMETRICS

Face Recognition

Biometrics technology has matured rapidly over recent years, and the use of it for security and authentication purposes has become increasingly common. Biometrics technology uses biological data to identify an individual by analyzing and measuring characteristics such as fingerprints, DNA, iris and other unique attributes of a person.

Due to recent advances in the reliability, accuracy and performance, face recognition is the latest biometric technology to 'come of age'. Unlike other forms of biometric solutions, face recognition requires no physical or deliberate interaction by the subject, making it one of the more passive and less intrusive forms of biometrics.

Speed, accuracy and reliability are the main features required of a face recognition solution. Identifying people on a pre-defined watch list needs to happen without delay every time there is a near precise match. But a successful deployment of face recognition needs to consider a number of factors beyond the physical hardware and software. Lighting conditions, angles, aging, facial expressions and obstructions such as hats and facial hair, all need to be taken into account, along with calculating the required processing power and capture rates particularly if being used in a busy or crowded environment.

Like most biometrics technologies, security and public safety uses have been the driving factor behind the development and adoption of face recognition for verifying or identifying individuals. But the commercial sector is also beginning to see the potential gains to be had in recognizing an individual without the need for any interaction. Consequently, face recognition is being considered in a growing number of commercial applications which utilize the authentication and monitoring capabilities for less critical deployments.

NEC has years of experience in developing and deploying biometric technologies for security and commercial based applications across a variety of environments. This understanding of both the technology and the challenges has led to the creation of a series of face recognition applications that utilize NEC's market leading 'Neo-face' face recognition software.



Commercial Applications

Harvesting the benefits of face recognition for non-security based uses can provide organisations with a number of benefits in terms of improving customer service and enhanced business intelligence, as well as offering a real competitive advantage.

The opportunities to use facial recognition in the hospitality, leisure and retail markets are endless. Forward thinking organisations in these markets are deploying facial recognition to enable discrete handling of VIPs and the prevention of undesirable visitors.



VIP IDENTIFICATION

In some businesses, identifying VIPs is important, whether it is to simply alert personnel to their presence or to automate access to a specific area for the VIP to improve the customer experience.

In other instances, the identification of a VIP in the database can trigger an alert or work process for personnel to perhaps provide some degree of special attention. The solution works by matching the captured image in the VIP database. Alerts can then be sent to key personnel, along with enhanced data on the individual.



QUEUE MONITORING

Queues are an annoyance to those in them, and a potential issue for responsible for the immediate environment around them.

The queue management solution measures the flow of individuals between multiple points, providing information on the number of individuals and the time between points. The system is configured with certain parameters, enabling it to monitor queuing times and estimate waiting times.

The solution can then trigger alerts to key personnel who can take remedial action such as opening new access or check points to help reduce queue lengths and times, improving the customer experience.

The solution can also help with monitoring public areas to alert when the area becomes too busy or overcrowded. Again alerts can be triggered to relevant personnel to take action to perhaps open more entry points or divert people to other areas, reducing the risk to public safety.



BUSINESS INTELLIGENCE

Face recognition can also be used to monitor, measure and collect data about people in a specific area to gather priceless intelligence to improve business activities and operations. For example, this can include counting people, age, gender, facial expressions and time in the area. This data can be collated and analyzed retrospectively or can even be used dynamically to trigger a real time event such as changing a message or content on digital signage.

Understanding more about the people in a specific area can help organisations to tailor activities to gain both commercial and customer experience benefits.



DETECTION OF UNWANTED INDIVIDUALS

One of the most common applications is identifying individuals in an open environment who provide a risk to public safety or a security risk or possibly are known trouble makers or offenders.

Using a watch-list database, face recognition can be used to identify these individuals quickly from the live CCTV footage or security surveillance cameras

The face recognition software does a quick look up in the black list database and where a match is found, alerts can be made to security personnel or staff both on screen in the control room as well as sending the information to the most appropriate personnel best placed to react, enabling a quick response to the threat.



ACCESS CONTROL

Face recognition can also be used for access control solutions. This can include physical building entry where face recognition is used as a pass or a part of the entry process and linked directly with a door or turnstile. A positive match in the database triggers the opening of the door or turnstile, allowing the individual entry. It can also be integrated into an automated registration kiosk for visitors.

In addition, access control can be applied to other items which require restricted access, including for example drugs cupboards.

In some instances, access control solutions can be combined with a second monitoring system to identify any other people trying to enter on the back of an approved individual.



Security Applications

NeoFace, face recognition can be used in a variety of security applications and environments for everyday tasks that can be automated, authenticated or enhanced, providing everyday people with a better quality of life and an improved level of security. Door access, retail, hospitality, border control, immigration, CCTV surveillance and law enforcement are just some of the areas NeoFace is being used worldwide.



SECURE AREA MONITORING

Secure area monitoring works in identifying individuals within a specific area. The solution monitors faces and positively matches them against a database which can include staff, contractors and visitors.

In this application, if an individual is not matched in the database, then they are instantly identified as a risk or threat. Alerts can then be made to security personnel or other staff either on a central control room screen or in the form a message sent to the most appropriate personnel best placed to react, enabling a quick response to the threat.

NEC

ABOUT NEC'S

Face Recognition

NEC's Face recognition is independently recognized as among the fastest and most accurate Face recognition software on the market place according to the latest tests done by the National Institute of Standards and Technology (NIST). The tests positioned NEC's face recognition software as the most accurate facial recognition software. These tests also demonstrated that NEC provides the fastest matching capability that is the most resistant to variants in angle, age and race.

Through the utilization of a unique matching face detection method, we are able to provide high speed and high accuracy for facial detection and facial features extraction. NEC's facial recognition relies on a modified Generalized Learning Vector Quantization (GLVQ) algorithm. GLVQ is not easily fooled by attempts to conceal identity through the usage of caps, hats or sunglasses.

THE SOFTWARE WORKS TO A 4 PART PROCESS:

1.

CAPTURE

The application takes in real time video from surveillance cameras, CCTV or archived video footage at a rate of up to 30 frames per second.

2.

ASSESS

The individual frames of video are each assessed, faces are detected and then each one analysed to determine its unique facial signature.

3.

MATCH

The software then undertakes a matching exercise against a watchlist database which includes enrolled images of individuals.

4.

REACT

A series of outcomes can be configured from a successful match. These outcomes or actions can be configured to happen if there is a positive match against one of the images in the database or on a negative match where someone is spotted who is not in the database.

NEC

World Leader in Biometrics

NEC is a world leader in biometric solutions. NEC's biometrics algorithms have been tested by the United States National Institute of Standards and Technology (NIST) and found to be among the best in the world. NEC was ranked most accurate in both single and multi-finger tests. NEC's algorithms were ranked among the top three in the one-to-one fingerprint matching tests and the two-finger matching tests. It consistently achieved top rankings in the lowest false

accept and the lowest false reject rates tests. In the automated latent print identification, NEC ranked first in all accuracy text categories. NEC's Face Recognition technology was also number one in the latest Biometric Grand Challenge's (MBGC) "Still Face Challenge", carried out by NIST in 2009. It also ranked highly in other related face recognition tests conducted by NIST.

Live, work and play in safety

'Safer Cities' is an integral part of NEC's vision for Smart Cities, where people are able to live, work, and play in safety and comfort while also coexisting in harmony with the environment.

The many disasters around us – natural and manmade – are vivid reminders of how complex and unpredictable the world has become. With improved communications capabilities, citizens today are better informed and enabled to make demands on government to respond more quickly to any safety or security breach.

NEC has decades of invaluable experience in delivering solutions across highly demanding and strategically vital environments. Through our Safer Cities initiatives, we harness cutting edge solutions and technologies to safeguard lives and assets in an increasingly unpredictable world.

With a proven track record across Asia Pacific, Latin America, Europe, North America, Middle East and Africa, NEC has a uniquely powerful platform which allows best practices to be shared across the globe meaningfully.

About NEC Global Safety Division

NEC Global Safety Division, a business division within NEC Corporation, spearheads the company's public safety business globally. The Division is headquartered in Singapore and offers solutions in the following domains: Citizen Services & Immigration Control, Law Enforcement, Critical Infrastructure Management, Public Administration Services, Information Management, Emergency & Disaster Management, Inter-Agency Collaboration. Leveraging on its innovative solutions, the Division aims to help government and business make cities safer.

NEC Global Safety Division

Global headquarters: No.1 Maritime Square #12-10, HarbourFront Centre, Singapore 099253
For enquiries, please contact safety@gsd.jp.nec.com

nec.com/safety

Facial recognition, once a battlefield tool, lands in San Diego County

Nov 07, 2013



Ali Winston
Contributor

READ THIS LATER

SHARE

Investigation(s):

Topic(s):



Officer Rob Halverson, with the Chula Vista Police Department in California, uses a Samsung Galaxy tablet to identify a woman as part of a pilot program in San Diego County testing facial recognition software.

Credit: Roque Hernandez/Univision

On a residential street in San Diego County, Calif., Chula Vista police had just arrested a young woman, still in her pajamas, for possession of narcotics. Before taking her away, Officer Rob Halverson paused in the front yard, held a Samsung Galaxy tablet up to the woman's face and snapped a photo.

Halverson fiddled with the tablet with his index finger a few times, and – without needing to ask the woman's name or check her identification – her mug shot from a previous arrest, address, criminal history and other personal information appeared on the screen.

Halverson had run the woman's photograph through the *Project Exile*, a new mobile facial recognition technology now in the hands of San Diego-area law enforcement. In an instant, the system matches images taken in the field with databases of

about 348,000 San Diego County arrestees. The system itself has nearly 1.4 million booking photos because many people have multiple mug shots on record.

The little-known program could become the largest expansion of facial recognition technology by U.S. law enforcement. Amid an international debate over collecting and sharing huge amounts of data on the public, this pilot program is putting that metadata to use in the field in real time.

The use of this technology was rolled out without any public hearings or notice. In turn, the secrecy of the program has alarmed privacy experts and raised questions about whether San Diego is the leading edge of an alarming future – one in which few people escape cataloging in a government database.

Twenty-five local, state and federal law enforcement agencies – including U.S. Immigration and Customs Enforcement, the Border Patrol, the San Diego County Sheriff's Department and San Diego State University – are part of the project. The project is coordinated by the San Diego Association of Governments and relies on a vast data-sharing program called the Automated Regional Justice Information System.

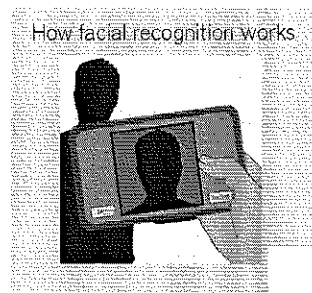
For some, the use of biometric technology by police represents a radical milestone in the militarization of American law enforcement.

For years, technology that was developed on the battlefield has been migrating into domestic police agencies. Since 9/11, America's wars in Afghanistan and Iraq have sped up that transfer. Facial recognition technology, which has been widely used by the military, is the next frontier.

"What we're seeing now is much more surveillance oriented, and it's in the guise of preventative policing," said Kevin Keenan, former executive director of the American Civil Liberties Union of San Diego & Imperial Counties. "It's really this aspiration of prevention and social control through the monitoring of everyone's every action and storage in perpetuity."

San Diego's program, if considered successful, easily could expand beyond the county's borders.

The system's mug shots are pulled from the statewide Cal-Photo law enforcement database, which also has access to 32 million driver's license photos. And, by the Automated Regional Justice Information System, the county is looking at using mug shots from statewide gang and parolee databases, as well as information stored by the Department of Motor Vehicles.



Click to view the full graphic.

The legality of law enforcement using facial recognition technology has not been tested in the courts. But a Privacy Impact Assessment, which the Automated Regional Justice Information System helped write, claims that photos of everyday people can be taken during "traditional police-civilian encounters."

San Diego law enforcement agencies have used the facial recognition system since the beginning of this year, when 133 Galaxy tablets and smartphones were distributed to 25 law enforcement agencies around the region, according to documents obtained through a public records request by the Electronic Frontier Foundation, a San Francisco nonprofit that studies surveillance and privacy issues.

Compared with the number of arrests throughout the San Diego region, which has about 3.2 million residents, the system is rolling out with relatively modest numbers. In the first 10 months of 2013, officers ran 5,629 queries through the database.

The sheriff's department and San Diego Police Department have the most devices, with 64 and 27 devices, respectively, and they have made nearly 2,000 queries into the system combined. The most active single user is an SDSU police officer who used a device 224 times from January to Oct. 30, according to the

documents.

Officials with the sheriff's department and San Diego Association of Governments declined requests for comment.

Law enforcement officials said the pilot program is a valuable tool to help them identify people who refuse to give their names or use fake identification. Immigration officials said they have used the system to help them when they encounter immigrants who don't have authorization to be in the U.S.

"Photographs are neutral – you can't say it's racist when a camera is taking a neutral picture of someone," said Halverson, the Chula Vista officer. "It's hitting on certain points of contact. It's doing a neutral analysis of a person."

The software works by capturing a freeze frame of a live video feed, which then focuses on the face and uses the distance between the eyes as a baseline. An algorithm then analyzes unique textures and patterns on the face, cross-referencing the freeze frame at the rate of a million comparisons per second against the police mug-shot database that also has been processed by the software.

Halverson said he has used the system to identify injured people who were unresponsive and had no identifying documents. Other officers have been overwhelmingly positive, according to the Automated Regional Justice Information System.

One Immigration and Customs Enforcement agent who provided a testimonial said he used the device during a warrant sweep in Oceanside. While on the sweep, the agent wrote, his "spidy senses" were tingling about the immigration status of a neighbor of the person he was pursuing.

He decided to run the man's picture through the facial recognition software. The agent discovered the man was in the country illegally and had a 2003 DUI conviction in San Diego.

"I whipped out the Droid (smartphone) and snapped a quick photo and submitted for search," the immigration agent wrote in his testimonial for the Automated Regional Justice Information System. "The subject looked inquisitively at me not knowing the truth was only 8 seconds away. I received a match of 99.96 percent. This revealed several prior arrests and convictions and provided me an FBI #. When I showed him his booking photo, his jaw dropped."

Law enforcement officials said the facial recognition software has built-in privacy safeguards. After an image taken in the field is run through the system, it is discarded by the central database, they said. They say it does not create a database of photos of people who are stopped by police and questioned.

"If you're not in a criminal database, you have nothing to hide," Halverson said.

However, during field tests with Chula Vista police, images taken by field officers were stored within individual tablets. It's up to police to delete those photos on their own.

Officers who have used the system in San Diego rave about its precision in identifying people. But facial

recognition technology remains imperfect. Documents obtained by the Electronic Privacy Information Center, a Washington nonprofit, show that the FBI's facial recognition program could fail to identify the right person in 1 out of 5 encounters – potentially ensnaring innocent people in investigations.

Developing the program

Development of the San Diego program goes as far back as 2007, according to documents obtained by the Electronic Frontier Foundation. That's when the federal government's National Institute of Justice awarded a \$418,000 information-led policing grant to the Automated Regional Justice Information System.

The program's goal, according to the proposal, was to develop open-source software that "will be made available as part of a repeatable national model." Over the next few years, the San Diego Association of Governments and county sheriff's department worked together to vet potential vendors and develop the system.

In 2012, the association selected FaceFirst LLC, a privately held facial recognition firm in Camarillo, Calif., as the technology vendor. A \$475,000 Department of Homeland Security grant covered the cost of purchasing FaceFirst's license and the hardware required to roll out the system.

Founded in 2007, FaceFirst is a spinoff of military contractor Airborne Technologies and is backed by the \$18 billion private equity firm Kayne Anderson Capital Advisors. FaceFirst's main product is facial recognition software that, according to CEO Joe Rosenkrantz, has the capability to "identify everyone in a football stadium in five seconds."

The \$126,800 contract for the San Diego system is the company's first public contract in the United States. Tocumen International Airport in Panama City also uses FaceFirst's technology. Rosenkrantz would not say whether the company's products are used by federal law enforcement, but the company has had talks with the Pentagon, Border Patrol and Navy.

During heavy fighting in Fallujah, Iraq, in 2007, the American-led coalition forces documented civilians they came into contact with in a database of mug shots, iris scans and fingerprints taken in the field with mobile devices, according to *Wired* magazine. The military has used facial recognition for virtually every Afghan it comes into contact with.

In 2009, Air Force Gen. Victor Renuart, the Pentagon's homeland security commander, advocated for the increased use of biometrics within the U.S. Among domestic law enforcement, the Maricopa County Sheriff's Office in Arizona and the Pinellas County Sheriff's Office in Florida have devoted considerable time and resources to developing biometric technology.

Jennifer Lynch, a senior staff attorney at the Electronic Frontier Foundation, expressed alarm at the normalization of military-grade technology in daily police activity. She said she believes the San Diego



San Diego law enforcement agencies have used the facial recognition system since the beginning of this year, when 133 Galaxy tablets and smartphones were distributed to around the region, according to the Electronic Frontier Foundation.

Credit: Roque Hernandez/Univision

regional government's lack of transparency around the facial recognition program is designed to minimize opposition and public debate.



"It becomes accepted and is much harder to push back when an agency has purchased 150 devices and deployed them in the field," Lynch said.

Biometrics is a multibillion-dollar-a-year industry, with more than 70 percent of spending by the military, domestic law enforcement and the government, according to the Los Angeles Times. Next year, the FBI will unveil its Next Generation Identification system, a nationwide database of biometric information on criminal suspects and convicts that will replace the bureau's current national database of fingerprints, corresponding criminal records and notes from past field interviews.

Keenan, the former San Diego ACLU official, pointed to the U.S.' history of political surveillance after World War II and 9/11 as evidence that the rapid proliferation of biometric technology is part of a tightening net of social control in the United States.

"We were given a false bargain," Keenan said. "We were told that this kind of control is to prevent another 9/11, and in fact, it's going to be used to fight the drug war, to pursue other policies where we would not have bargained away our privacy back at that time if we knew that was the tradeoff."

This story was edited by Robert Salladay and copy edited by Nikki Frick and Christine Lee.

 Chicago Police Department		Department Notice D13-11	
FACIAL RECOGNITION TECHNOLOGY			
			
ISSUE DATE:	23 August 2013	EFFECTIVE DATE:	23 August 2013
RESCINDS:			
INDEX CATEGORY:	Department Notice		

I. PURPOSE

This directive informs Department members of the availability of facial recognition technology for investigative purposes.

II. GENERAL INFORMATION

Facial recognition technology used by the Department accomplishes facial matching by creating a template of mapped geometric points from an existing image. The software uses an algorithm that maps the facial image and then compares it to those images within the comparison database. The software then ranks the highest scoring mugshots to the suspect image.

III. UNITS WITH FACIAL RECOGNITION TECHNOLOGY

Facial Recognition Technology (FRT) software is being used in the Bureau of Detectives - Area Detective Divisions, Bureau of Organized Crime, and Crime Prevention Information Center (CPIC).

IV. RESPONSIBILITIES

The Bureau of Detectives is responsible for investigative follow-up involving images for FRT. Policies, training and protocols will be developed and maintained by the Bureau of Detectives.

V. PROCEDURES

When preliminary investigating officers determine that photographic or video evidence exists that has a facial image that might be identified through FRT they will:

- A. Notify the responsible Area Detective Unit.
- B. If requested, prepare a supplementary report informing followup investigators that an image is available and whether it has been inventoried. If the image has been inventoried, provide the inventory number of the evidence.
- C. Inform the Area Detective Unit where the image may be located if the digital evidence has not been inventoried. Notification will be recorded in their Automated Incident Reporting Application (AIRA) report..

Garry F. McCarthy
Superintendent of Police

13-067 RWN

Get short URL



an article this week. The FBI first outlined the project back in 2005, explaining to the Justice Department in an August 2006 document (.pdf) that their new system will eventually serve as an upgrade to the current Integrated Automated Fingerprint Identification System (IAFIS) that keeps track of citizens with criminal records across America .

"The NGI Program is a compilation of initiatives that will either improve or expand existing biometric identification services," its administrator explained to the Department of Justice at the time, adding that the project, *"will accommodate increased information processing and sharing demands in support of anti-terrorism."*

"The NGI Program Office mission is to reduce terrorist and criminal activities by improving and expanding biometric identification and criminal history information services through research, evaluation and implementation of advanced technology within the IAFIS environment."

The agency insists, *"As a result of the NGI initiatives, the FBI will be able to provide services to enhance interoperability between stakeholders at all levels of government, including local, state, federal, and international partners."* In doing as such, though, the government is now going ahead with linking a database of images and personally identifiable information of anyone in their records with departments around the world thanks to technology that makes fingerprint tracking seem like kids' stuff.

According to their 2006 report, the NGI program

UTILIZES *specialized requirements in the Latent Services, Facial Recognition and Multi-modal Biometrics areas*" that *"will allow the FnewBI to establish a terrorist fingerprint identification system that is compatible with other systems; increase the accessibility and number of the IAFIS terrorist fingerprint records; and provide latent palm print search capabilities."*

Is that just all, though? During a 2010 presentation (.pdf) made by the FBI's Biometric Center of Intelligence, the agency identified why facial recognition technology needs to be embraced. Specifically, the FBI said that the technology could be used for *"Identifying subjects in public datasets,"* as well as *"conducting automated surveillance at lookout locations"* and *"tracking subject movements,"* meaning NGI is more than just a database of mug shots mixed up with fingerprints — the FBI has admitted that this their intent with the technology surpasses just searching for criminals but includes spectacular surveillance capabilities. Together, it's a system unheard of outside of science fiction.

New Scientist reports that a 2010 study found technology used by NGI to be accurate in picking out suspects from a pool of 1.6 million mug shots 92 percent of the time. The system was tested on a trial basis in the state of Michigan earlier this year, and has already been cleared for pilot runs in Washington, Florida and North Carolina. Now according to this week's New Scientist report, the full rollout of the program has begun and the FBI expects its intelligence infrastructure to be in place across the

United States by 2017.

In 2008, the FBI announced that it awarded Lockheed Martin Transportation and Security Solutions, one of the Defense Department's most favored contractors, with the authorization to design, develop, test and deploy the NGI System. Thomas E. Bush III, the former FBI agent who helped develop the NGI's system requirements, tells NextGov.com, *"The idea was to be able to plug and play with these identifiers and biometrics."* With those items being collected without much oversight being admitted, though, putting the personal facts pertaining to millions of Americans into the hands of some playful Pentagon staffers only begins to open up civil liberties issues.

Jim Harper, director of information policy at the Cato Institute, adds to NextGov that investigators pair facial recognition technology with publically available social networks in order to build bigger profiles. Facial recognition *"is more accurate with a Google or a Facebook, because they will have anywhere from a half-dozen to a dozen pictures of an individual, whereas I imagine the FBI has one or two mug shots,"* he says. When these files are then fed to law enforcement agencies on local, federal and international levels, intelligence databases that include everything from close-ups of eyeballs and irises to online interests could be shared among offices.

The FBI expects the NGI system to include as many as 14 million photographs by the time the project is in full swing in only two years, but the pace of technology and the new connections

constantly created by law enforcement agencies could allow for

a database that dwarfs that estimate. As RT reported earlier this week, the city of Los Angeles now considers photography in public space "suspicious," and authorizes LAPD officers to file reports if they have reason to believe a suspect is up to no good. Those reports, which may not necessarily involve any arrests, crimes, charges or even interviews with the suspect, can then be filed, analyzed, stored and shared with federal and local agencies connected across the country to massive data fusion centers. Similarly, live video transmissions from thousands of surveillance cameras across the country are believed to be sent to the same fusion centers as part of TrapWire, a global eye-in-the-sky endeavor that RT first exposed earlier this year.

"Facial recognition creates acute privacy concerns that fingerprints do not," US Senator Al Franken (D-Minnesota) told the Senate Judiciary Committee's subcommittee on privacy, technology and the law earlier this year. *"Once someone has your faceprint, they can get your name, they can find your social networking account and they can find and track you in the street, in the stores you visit, the government buildings you enter, and the photos your friends post online."*

In his own testimony, Carnegie Mellon University Professor Alessandro Acquisti said to Sen. Franken, *"the convergence of face recognition, online social networks and data mining has made it possible to use publicly available data and inexpensive technologies to produce sensitive inferences merely starting from an anonymous face."*

"Face recognition, like other information technologies, can be source of both benefits and costs to society and its individual members," Prof. Acquisti added. "However, the combination of face recognition, social networks data and data mining can significant undermine our current notions and expectations of privacy and anonymity."

With the latest report suggesting the NGI program is now a reality in America, though, it might be too late to try and keep the FBI from interfering with seemingly every aspect of life in the US, both private and public. As of July 18, 2012, the FBI reports, *"The NGI program ... is on scope, on schedule, on cost, and 60 percent deployed."*

A Practical Application: Facial Recognition Technology

By Owen McShane, Director, Division of Field Investigation, New York State Department of Motor Vehicles; and Anne Dowling, Deputy Director, Institute for Traffic Safety Management and Research, State University of New York, University at Albany, New York

The key to a state having a secure driver license and identification card issuance system is a comprehensive approach that focuses on prevention and deterrence against fraud. From the initial application process to the final document issuance, it is important that the system focuses on ensuring that the applicants are "who they say they are." Over the past 10 years, the New York State Department of Motor Vehicles (NYSDMV) has implemented a variety of new programs and initiatives to help ensure this process, such as electronically verifying the social security numbers for all license applications and installing new verification machines that help verify breeder documents that are used to establish a customer's identity.

Cutting-edge Technology

During the past three years the NYSDMV process has taken an important leap forward with the implementation of cuttingedge facial recognition technology. The new facial recognition program is intended to advance the NYSDMV's important goal of "one driver, one license" to deter identity fraud and improve highway safety.

Under a \$2.5 million grant from the U.S. Department of Homeland Security, NYSDMV's Division of Field Investigation (DFI) initiated an effort in 2010 to incorporate facial recognition technology into its business practices for the primary purpose of preventing and deterring the issuance of multiple licenses to a single individual. This important undertaking involves searching New York's driver license file of approximately 21 million records (all with facial images) for duplicate records and for drivers with multiple licenses or identities. To accomplish this, NYSDMV is using facial recognition technology in a dual manner: (1) to compare existing images on the driver license file for possible matches, and (2) to compare a new image from a prospective license applicant to the existing file of facial images before issuing a license document. This ensures that no more than one document is issued to an applicant. These two uses of facial recognition technology are important to NYSDMV in stopping identity theft and driver license fraud.

Origin of Multiple License Records

The problem of multiple records on the NYSDMV driver license file for a single individual has many origins. Some multiple records are the result of simple data entry mistakes by the reporting agencies involved (for example, law enforcement agencies and courts) and by the NYSDMV data entry staff itself. Some are the result of transactions involving name changes stemming from marriage and divorce. However, investigations have revealed that many multiple records on the DMV database are the result of a deliberate effort to circumvent various laws and possible sanctions or penalties for violation of those laws, including New York's Vehicle and Traffic Law, tax law, social service laws, and penal laws.

With a goal of having one record for each driver (that is eliminating the creation of multiple licenses per individual), NYSDMV has identified three distinct groups who attempt to establish a second identity or maintain multiple identities:

Group 1: Individuals engaged in identity theft or other criminal acts.

Group 2: Individuals wanted under their true identity who establish a second name as an alias. This group poses a high risk for law enforcement encounters because officers may believe they are dealing with a first time traffic offender when they are actually dealing with a wanted felon.

Group 3: Individuals who have multiple traffic violations (for example, traffic infractions, DWIs, insurance suspensions) who establish an alias in order to (1) continue to appear to drive legally while suspended under their true identities, or (2) avoid suspensions by dividing tickets and infractions among multiple records.

Each of these three groups represents a serious problem, albeit from different perspectives. The first two groups involve individuals who pose a serious risk to the general public's safety, which requires action by the state's law enforcement community. In comparison, the third group poses a serious risk to those using New York's roadways, which requires the attention of the state's traffic safety community. Since research has consistently shown that driver behavior is a key contributing factor in the large majority of traffic crashes, the issue of a single person having multiple licenses or records has serious traffic safety implications.

Since NYSDMV is concerned with both the public safety and traffic safety issues related to multiple licenses, in January 2010, the Institute for Traffic Safety Management and Research, a not-for-profit research center affiliated with the University at Albany, was asked to assist the DFI in examining and analyzing the records of persons across the state who have or are trying to obtain more than one driver license or non-driver identification (ID) card.

Using Facial Recognition Technology

A two-pronged approach is being used in the statewide roll out of the facial recognition program. One approach takes all of the photos that are captured daily by NYSDMV's offices across the state and conducts a one-to-one comparison against older photos of the subject, followed by a one-to-many search against all the other photos in the NYSDMV's database. Approximately 7,000 customer photos are taken daily and compared to the more than 21 million driver and nondriver ID photos in the database. The second approach, also conducted on a daily basis, takes a percentage of the "legacy" photos and conducts a one-to-many search of the other photos. Due to the size of the legacy file, this second approach took three years to complete.

When the investigation of the identified "matched records" is complete, the records are merged, as warranted. The merged record is then reviewed to determine whether the individual's license should be suspended or revoked based on the combined number of tickets, points, open suspensions, crashes, and so forth that are on the merged record.

The results of the matching process for the first two years of the program, February 3, 2010, to February 2, 2013, from both a public safety perspective and a traffic safety perspective, are summarized below.

Public Safety Implications

The primary objectives of implementing the use of facial recognition technology are to identify individuals

- engaged in identity theft or other criminal acts, and
- individuals wanted under their true identity who establish a second name as an alias.

These issues are significant, especially identity theft, as it is a serious crime that affects 11 million people nationally in any given year, which suggests that 1 in 20 U.S. citizens are at risk of becoming a victim.

Over the three-year period, more than 21 million photos were compared using the facial recognition technology. Overall, this resulted in over 13,500 cases being generated for subjects that had two or more records with NYSDMV. The system also identified 7,710 potential matches, which were determined to be twins or multiple births.

While investigations of the more than 13,000 possible fraud cases are ongoing, key findings of the first three years of operation include the following:

- More than 2,500 felony arrests were made, including
 - A subject holding four New York licenses under separate names, who was also naturalized as a U.S. citizen under the same names and was issued four different valid Social Security numbers. The subject was found to be on the no-fly list under the name he used when he initially settled in the United States.
 - Over 250 Commercial Driver License (CDL) drivers were found to have two or more licenses. Many of these drivers had open suspensions, DWI charges, and convictions for other offenses that would have prevented them from obtaining a CDL license under their "true" names.
 - A subject who had multiple active warrants under his true name since 1993 for bank robbery who was arrested after the photo from his new identity matched his old

license record, which was still suspended for unpaid moving violations.

- In addition, administrative action was initiated on more than 7,000 individuals who were identified as having multiple records where the license transactions were too old for criminal prosecution. Generally, the subject's license would be revoked for a one-year period and all records for the subject would be merged. In this way, subjects would be held accountable for all tickets or accidents they had accumulated under the different identities they had used.

Traffic Safety Implications

Although the use of facial recognition technology is gaining popularity among the state's driver licensing agencies to prevent and deter driver license fraud, the use of such technology to identify traffic safety-related problems is limited. The primary issues related to individuals with multiple license records is the extent to which they are obtaining multiple licenses to hide the fact that they have multiple traffic violations or multiple crashes on their driving records. Obtaining and using multiple license records in this manner enables a driver to avoid the appropriate sanctions and penalties associated with such events. As a result, problem drivers remain on the state's roadways, putting other highway users at risk.

To study the traffic safety implications of multiple records, 6,111 cases of "matched records" with possible fraud problems, from the first two years of the program, were reviewed and analyzed to identify how individuals are using their multiple records and determine whether their use has traffic safety implications. Key findings from the review to date show the following:

- 21 percent (1 in 5 subjects) did not have a valid license.
- 3 percent had been involved in a crash, compared to 42 percent of all New York state (NYS) licensed drivers.
- 9 percent had been convicted of impaired driving, compared to 2 percent of all NYS licensed drivers.
- 29 percent had been convicted of a cellphone violation compared to 9 percent of all NYS licensed drivers.
- 56 percent had been convicted of a seat belt violation compared to 21 percent of all NYS Licensed Drivers.
- 35 percent had accumulated six or more points on their license record within an 18-month period at some point in time after November 18, 2004, compared to 11 percent of all NYS licensed drivers.

The Future

The NYSDMV is very excited about its successful use of facial recognition technology to uncover identity fraud and keep its highways safer. The total success of this program relies on the ongoing cooperation among the state's traffic safety organizations, law enforcement personnel, and prosecutors.

The results of the facial recognition program are being shared with other federal and state agencies in an effort to combat fraud, especially among agencies that provide benefits. It is expected that the results of NYSDMV's facial recognition program will help these agencies uncover related fraud specific to their missions, such as the double collection of medical benefits, fraudulent tax refund applications, and improper disability claims. In the first three years of the program, the NYSDMV DFI identified subjects collecting benefits under multiple identities, as well as subjects working full time under one identity while collecting full disability under a second identity.

The knowledge gained to date from the program, together with the size of the New York driver's license file (approximately 21.5 million records with facial images), provides an unprecedented opportunity to explore the feasibility of using facial recognition technology to identify and address both public safety and traffic safety-related issues. ♦


Please cite as:

Owen McShane and Anne Dowling, "A Practical Application: Facial Recognition Technology," *The Police Chief* 80 (June 2013): 42-44.

[Top](#)

International Association of Chiefs of Police, 515 North Washington Street,
Alexandria, VA 22314 USA.

[Return to Article](#)

send to a friend 

The official publication of the International Association of Chiefs of Police.

The online version of the Police Chief Magazine is possible through a grant from the IACP Foundation. To learn more about the IACP Foundation, click here.

All contents Copyright © 2003 - 2015 International Association of Chiefs of Police. All Rights Reserved.

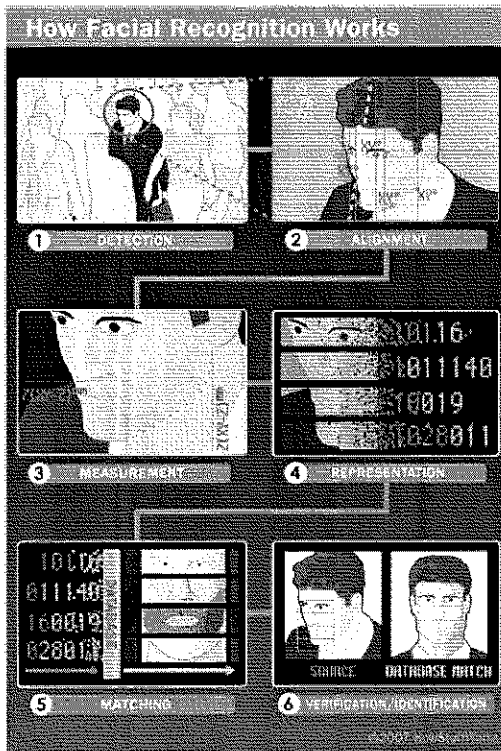
Copyright and Trademark Notice | Member and Non-Member Supplied Information | Links Policy

44 Canal Center Plaza, Suite 200, Alexandria, VA USA 22314 phone: 703.636.6767 or 1.800.THE IACP fax: 703.636.4543

Created by Matrix Group International, Inc.®

The top 6 FAQs about facial recognition

December 8th, 2011 by Sarah A. Downey



How facial recognition works. Via
HowStuffWorks.com.

With the FTC currently focusing on facial recognition, we figured it was a good time to provide answers to the 6 biggest questions about this technology and how it affects you.

1. What is facial recognition?
2. How is facial recognition being used today?
3. Can I be recognized? How?
4. What can I do about this?
5. What are the risks of facial recognition?
6. What are the benefits?

A stranger snaps a picture of you with his iPhone camera while you're walking down the street on your way to work in the morning. You don't see him. He uses a mobile app to analyze the photo he just took of you. The app scans your face and searches the web for matches. In less than a minute, the stranger knows your name and contact info, is scrolling through your Facebook albums, and is reading your Twitter timeline. Predicting your social security number—and thus stealing your identity—is one small step away.

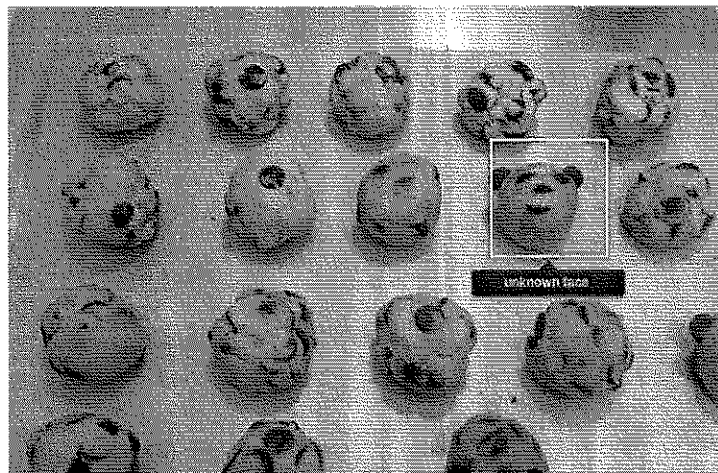
Your face is your identity: you should have control over it.

Sounds like science fiction? It's science fact. Say hello to the faceprint, the facial equivalent of the fingerprint. The identifying characteristics unique to our bodies are called biometrics. Iris patterns, faces, and fingerprints are common examples. Once you have a faceprint, you can compare it to a database of faces and look for a match. This is the world of facial recognition technology, and it's happening right now.

Frequently Asked Questions about Facial Recognition

1. What is facial recognition?

When we talk about facial recognition, we're really talking about two different applications: basic and advanced. Basic facial recognition answers the question, "Is this a face?" You see this kind of technology in photo-editing software. Apple's iPhoto is notorious for identifying non-faces, like cookies and animals, as faces. If it has eyes, a nose, and a mouth, there's a good chance it's a face.



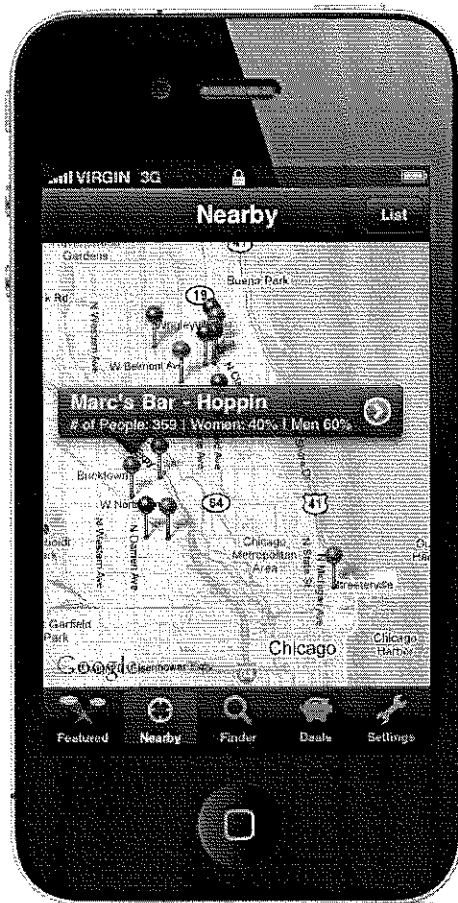
Who IS this guy?

Advanced facial recognition builds on these principles to answer the question, "Is this *a particular* face?" As anyone who's ever used a character builder in a video game can tell you, our unique faces are comprised of variations on several main features: the width of our nose, the wideness of our eyes, the depth of our jaw, the height of our cheekbones, and the distance between our eyes are a few of them. Facial recognition software takes your features and turns them into a numerical code. Compare this code, or faceprint, with any database of photos, and you can start making matches and identifications.

2. How is facial recognition being used today?

Facial recognition is alive and flourishing. It's used in many broad areas, including social networking, photo editing, security, law enforcement, casinos, and in odd places that you might not expect. For example, the dating website FindYourFaceMate.com based matchmaking around the principle that people with similar facial features are attracted to each other, using facial recognition to match user photos, and DoggelGanger.com matches potential dog owners with canines that look like them. Face recognition cameras scanned all the fans walking

through the turnstiles at Super Bowl XXXV, now referred to as the Snooper Bowl, running the scans against a database of criminal mugshots. That was a decade ago, when the internet was still in its relative childhood. We're in an age now when Facebook collects 100-page dossiers on all of us, when ad networks track everything we do online, when companies buy and sell our contact information: the street we grew up on, the names of our family members, aerial shots of our homes.



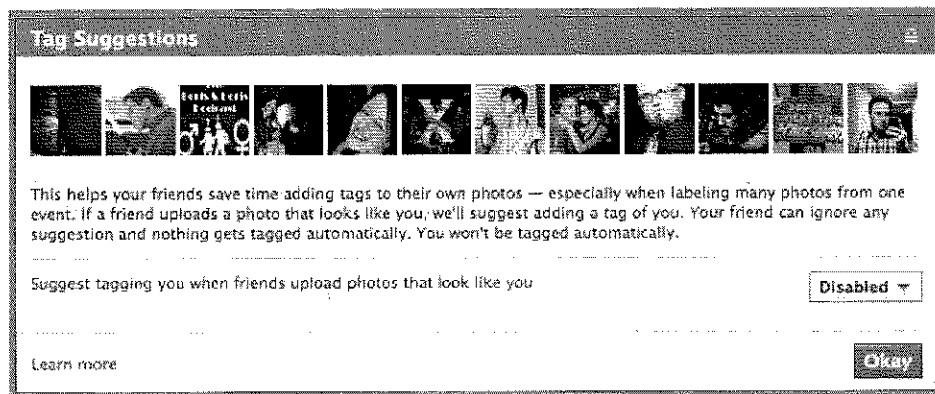
SceneTap's interface. The app lets you check the gender ratio of a bar before you head over.

Lots of mobile apps use facial recognition, too. A particularly interesting one, SceneTap, tracks the ratios of males to females and ages at 250 participating U.S. bars. These bars install face-detection cameras, and the app calculates the number of people at the bar, the male-to-female ratio, and the average age of patrons. SceneTap doesn't receive bar patrons' permission to capture their faces and share demographic information about them. Another notable app is FACER Celebrity, made by Animetrics Inc., a facial-recognition company based in Conway, N.H., that focuses on the law-enforcement and security industries. FACER Celebrity is a free iPhone app that allows users to match their face to a star. The app, which has about 30,000 downloads, uses the same facial-recognition technology deployed by local law enforcement to identify criminal suspects, says Animetrics CEO Paul Schuepp.

Companies give two main reasons for using facial recognition technology: it helps with security, and it makes photo editing and sharing easier. On the security side, law enforcement officials have argued that facial recognition can help find missing people, identify criminals in a crowd, preempt terrorists from boarding planes with fake passports. It's also used for private security in casinos to identify card counters and kick them out before they can win too much. Casinos also say their systems identify people with gambling addictions who've asked casinos to forcibly remove them if they can't stop themselves. Even supermarket security uses facial recognition: one grocery chain in the UK uses facial recognition to stop underage customers from buying alcohol.

On the photo sharing side, facial recognition can scan albums for faces and either suggest tags or automatically tag people. You'll already find it in Apple's iPhoto, Google's Picasaweb, Microsoft's Windows Live Photo Gallery, and other photo editors. It also collects information on different people's faces through existing tags: the more tags, angles, lighting types, hairstyles, and other details in your photos, the better the software's ability to pick you out in other photos. It's one thing to confine this technology to the photos on your own computer, but things get more complicated when the internet gets involved.

Facebook got in trouble with privacy advocates when it rolled out facial recognition by default. It's since dialed it back to "Tag Suggestions," which you can choose to disable. Even if you disable it, though, Facebook still collects information about your face whenever it's tagged. And when you consider that Facebook's 600 million members upload over 250 million photos every day, you see that they're building an empire of facial data. Rumor has it they're building a way to search for people by picture alone. And Google's Goggles app can already identify inanimate objects through photographs. Add already-existing facial recognition software to that, and you could "identify strangers on the street."



We recommend disabling tag suggestions in Facebook.

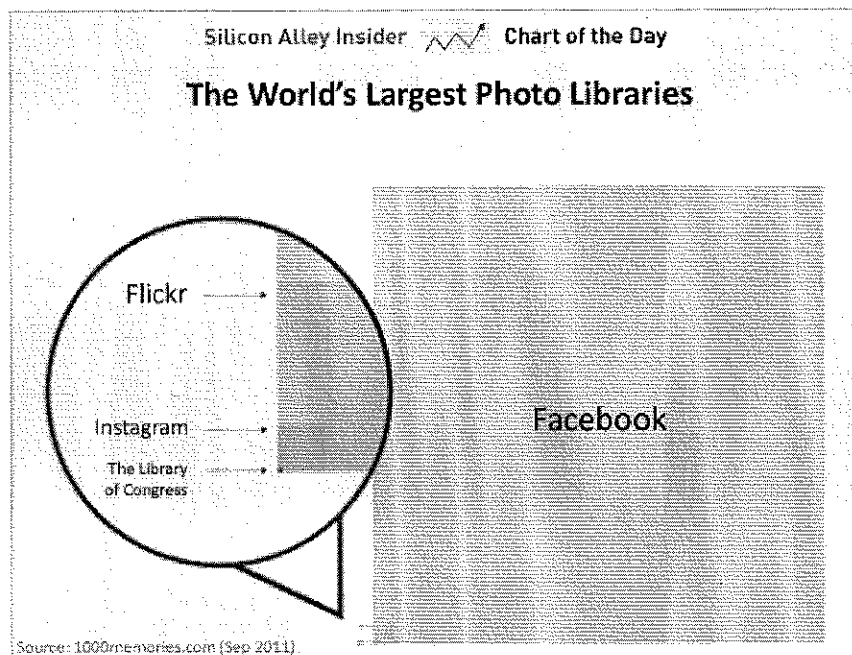
3. How accurate is it?

The accuracy rate is 99.31% on still frontal face images. Changes in lighting, face positioning, makeup, hairstyle, facial hair, glasses, and other accessories decreases the accuracy rate.

4. Can I be recognized? How?

Yes, as long as you have at least one picture of your face publicly available online. And yes, social networks count as "public" in most cases. The more photos there are of you on the internet, the greater the chances of the facial recognition software finding a match.

If someone took a picture of you while you are out on the street, they can scan it and cross-reference it against photo databases to get a match. You might guess that the U.S. Department of State has one of the biggest facial recognition databases with over 75 million photographs, but it doesn't come close to the largest of them all: Facebook, with over 140 billion photos (and it will add 70 billion more this year). That's up from 10 billion in 2008, and it makes up 4% of all photos ever taken throughout history. ImageShack has over 20 billion; PhotoBucket has 7.2 billion, Flickr has 3.4 billion.



Bet you didn't realize exactly how many photos Facebook has on its servers.

You can also be found through existing photos of yourself with reverse image searches such as TinEye or Google. Reverse image search works by looking for photo fingerprints, exact matches of existing photos. Merely similar photos won't show up, but cropped and differently-sized versions of the same photo will.

Let's say you're a member of an online dating site, and although you use a real photo of yourself, you don't provide your real name. If you've ever used that same photo anywhere else, you may be in trouble: anyone can save that picture and do a reverse image search with it. These searches reveal other locations where that photo can be found. Maybe it's your personal website, your Facebook profile, a people search website aggregating data about you, and a newspaper article. Suddenly, that person knows far more about you than you provided in your dating profile's "about me" section.

If you're worried about reverse image search, here's a tip: **use different images for different**

contexts. Don't use the same photo on your employer's profile page that you have as your Facebook profile picture. Keep separate photos you use for work, photos you use for family, photos you use for friends, and photos you want to keep entirely private. That way, someone doing a reverse search with a particular image will only find a limited set of results: the ones you've chosen to associate with that image.

5. What are the risks of facial recognition?

Take the massive amount of information that Google, Facebook, ad networks, data miners, and people search websites are collecting on all of us; add the info that we voluntarily provide to dating sites, social networks, and blogs; combine that with facial recognition software; and you have a world with reduced security, privacy, anonymity, and freedom. Carnegie Mellon researchers predict that this is "a world where every stranger in the street could predict quite accurately sensitive information about you (such as your SSN, but also your credit score, or sexual orientation)" just by taking a picture.

Risk 1: Identity theft and security

Think of your personal information—name, photos, birthdate, address, usernames, email addresses, family members, and more—as pieces of a puzzle. The more pieces a cyber criminal has, the closer he is to solving the puzzle. Maybe the puzzle is your credit card number. Maybe it's the password you use everywhere. Maybe you're your social security number.



Identity thieves often use social security numbers to commit fraud. Photo: listverse.com.

Facial recognition software is a tool that can put all these pieces together. When you combine facial recognition software with the wealth of public data about us online, you have what's

called “augmented reality:” “the merging of online and offline data that new technologies make possible.” You also have a devastating blow to personal privacy and an increased risk of identity theft.

Once a cyber criminal figures out your private information, your money and your peace of mind are in danger. Common identity theft techniques include opening new credit cards in your name and racking up charges, opening bank accounts under your name and writing bad checks, using your good credit history to take out a loan, and draining your bank account. More personal attacks may include hijacking your social networks while pretending to be you, reading your private messages, and posting unwanted or embarrassing things “as” you.

The research: how facial recognition can lead to identity theft

Carnegie Mellon researches performed a 2011 facial recognition study using off-the-shelf face recognition software called PittPatt, which was purchased by Google. By cross-referencing two sets of photos—one taken of participating students walking around campus, and another taken from pseudonymous users of online dating sites—with public Facebook data (things you can see on a search engine without even logging into Facebook), they were able to identify a significant number of people in the photos. Based on the information they learned through facial recognition, the researchers were then able to predict the social security numbers of some of the participants.

They concluded this merging of our online and offline identities can be a gateway to identity theft:

If an individual's face in the street can be identified using a face recognizer and identified images from social network sites such as Facebook or LinkedIn, then it becomes possible not just to identify that individual, but also to infer additional, and more sensitive, information about her, once her name has been (probabilistically) inferred.

Some statistics on identity theft from the Identity Theft Assistance Center (ITAC):

- 8.1 million adults in the U.S. suffered identity theft in 2011
- Each victim of identity theft loses an average of \$4,607
- Out-of-pocket losses (the amount you actually pay, as opposed to your credit card company) average \$631 per victim
- New account fraud, where thieves open new credit card accounts on behalf of their victims, accounted for \$17 billion in fraud
- Existing account fraud accounted for \$14 billion.

Risk 2: Chilling effects on freedom of speech and action

Facial recognition software threatens to censor what we say and limit what we do, even offline. Imagine that you're known in your community for being an animal rights activist, but you secretly love a good hamburger. You're sneaking in a double cheeseburger at a local restaurant when, without your knowledge, someone snaps a picture of you. It's perfectly legal for someone to photograph you in a public place, and aside from special rights of publicity for big-time celebrities, you don't have any rights to control this photo. This person may not have any ill intentions; he may not even know who you are. If he uploads it to Facebook, and Facebook automatically tags you in it, you're in trouble.



Anywhere there's a camera, there's the potential that facial recognition is right behind it.

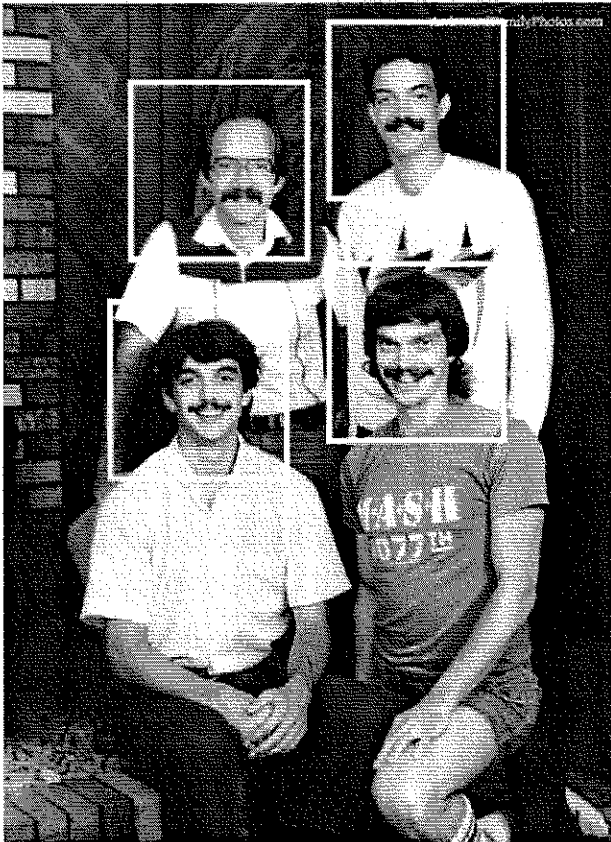
The same goes for the staunch industrialist caught at the grassroots protest; the pro-life female politician caught leaving an abortion clinic; the CEO who has too much to drink at the bar; the straight-laced lawyer who likes to dance at goth clubs. If anyone with a cell phone can take a picture, and any picture can be tied back to us even when the photographer doesn't know who we are, we may stop going to these places altogether. We may avoid doing anything that could be perceived as controversial. And that would be a pity, because we shouldn't have to.

Risk 3: Physical safety and due process

Perhaps most importantly, facial recognition threatens our safety. It's yet another tool in stalkers' and abusers' arsenals. See that pretty girl at the bar? Take her picture; find out everything about her; pay her a visit at home. It's dangerous in its simplicity.

There's a separate set of risks from facial recognition that *doesn't* do a good job of identifying targets: false identifications. An inaccurate system runs the risk of identifying, and thus detaining or arresting, the wrong people. Let's say that an airport scans incoming travelers' faces to search for known terrorists. Their systems incorrectly recognize you as a terrorist, and you're detained, searched, interrogated, and held for hours, maybe even arrested. This is precisely why Boston's Logan Airport abandoned its facial recognition trials in 2002: its systems could only identify volunteers 61.4 percent of the time.

6. What are the benefits of facial recognition?



Sometimes facial hair throws off facial recognition software. Too bad there's not mustache recognition software. Photo: AwkwardFamilyPhotos.com

Facial recognition has its benefits, especially for certain groups and activities.

Benefit 1: Easier photo organization

Facial recognition boasts the end of long tagging sessions. If you upload all your photos and facial recognition software identifies and tags your friends, most of your work is done. Even less powerful software that only identifies and suggests tags, rather than tags automatically, can save a lot of time.

Benefit 2: Greater access to information

If a picture's worth a thousand words, then a picture associated with a database of internet data is worth an encyclopedia. You could learn all about someone with a single photo. This could be helpful for people who need a lot of information in a short period of time: for example, if you want to learn about a potential

date, get some background on a job applicant, or find a long-lost friend or relative.

Facial recognition applications could have special significance for those with prosopagnosia, also known as face blindness. This condition makes it difficult or impossible to identify people. You may have met someone a hundred times, but if you have severe prosopagnosia, you won't recognize him or her. And for those of us who just have trouble remembering faces, this

wouldn't be a bad thing, either.



People with severe prosopagnosia can't recognize faces.

Photo: BodyGeeks.com

Benefit 3: Criminal identification

If you have a database of known criminals, you can use facial recognition to cross-reference those faces against other databases of faces. With the right technology, you could scan a public area for wanted felons, for example, or see if any of them have signed up for Facebook. Even if you can try to hide from a criminal past by changing your name, it's much harder to change your face. Thus facial recognition is already a valuable tool in law enforcements' arsenal, and it's only becoming more important.

Benefit 4: Money, money, money

If you're an advertiser, there's money in facial recognition. Photos are the key to unlocking a vault of valuable personal information. The more they know about a person or a segment, the better they can tailor their ads to target them, and the more successful these ads will be. Your data is worth its weight in gold.

What do you think about facial recognition?

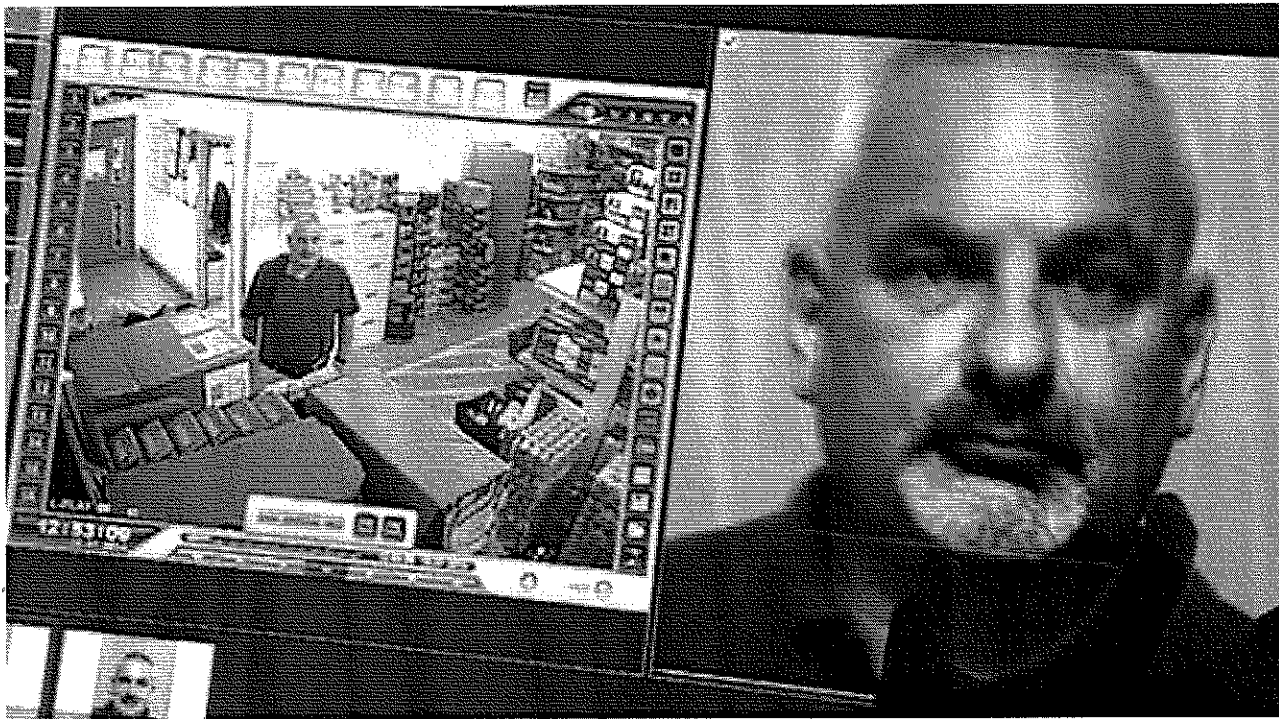
Is it cool? Scary? A little of both? What would you like to see happen with it in the future? Leave your thoughts in the comments box below.

About Abine: Abine, Inc., The Online Privacy Company, is the leading provider of online privacy solutions for consumers. Abine's products and services allow regular people to regain control over their personal information while continuing to browse, interact, and shop online.

UK, the world's most surveilled state, begins using automated face recognition to catch criminals

By [Sebastian Anthony](#) on July 17, 2014 at 8:03 am

26 Comments



Share This Article

1.1K

89

22

Police in the UK have become one of the first major police forces to deploy automated facial recognition technology to catch criminals. The British police will be using NEC's NeoFace technology, which

can match faces from crime scene photos or videos against a database of images in just a few seconds. Combined with the highest density of CCTV cameras of any country in the world, police body-worn cameras that are constantly recording, and a CSI-like smartphone and tablet app that allows for face and fingerprint matching in the field, it is rather hard to be a criminal in the UK nowadays.

Most modern police forces, including the FBI, have some kind of computerized face-matching system — but it involves laboriously looking through dozens of potential matches manually. NEC's NeoFace, which was released last year and has since been deployed by a few police forces, is fully automated, highly accurate, and very fast. The FBI isn't far behind with its own automated Next-Generation Identification (NGI) system, which has been slowly rolling out over the last couple of years (it's expected to turn on fully this summer). The NGI database, containing millions of fingerprints, faces, and other biometric records, will eventually be shared with all federal, state, and local police forces in the US.



Some happy British police, using NeoFace. Amusingly the NeoFace app appears to be running in the Windows 8 Metro interface.

NEC's NeoFace and the FBI's NGI both work in roughly the same way. The most important thing is that you need a big database of images to begin with — which, fortunately, the police is in possession of. The software goes through each of these images (potentially millions of them) and encodes them into specially tagged and formatted files. These files don't store image data, but rather biometric data — the distance between the eyes, the length of the nose, etc. Many of these images will already be associated with a criminal's police record, but that's not a requirement. Later, to find a match, the investigator simply feeds a new image into the system — a photo, a still from a crime scene video — and the same encoding/tagging process occurs. It is then a very quick process to compare the biometric markers from the new image against the entire database.

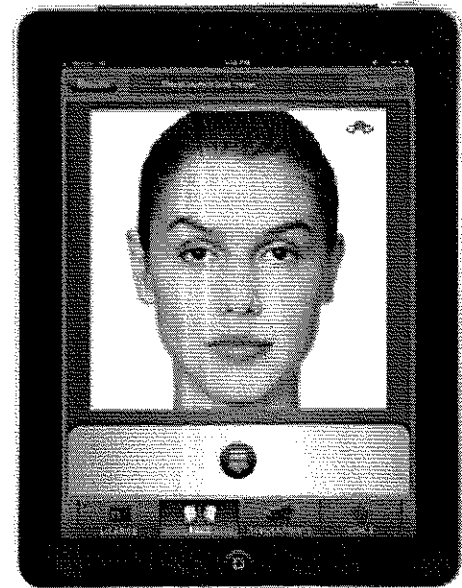
In the case of NeoFace, there are also a couple of companion apps. NeoFace Watch watches surveillance footage, constantly picking faces out of a crowd — and then storing those faces in a database, or matching them against a predefined watch list. NeoFace Smart ID is a smartphone and tablet app that allows for the real-time collection and identification of fingerprints, faces, voices, and other identifiable data at crime scenes.

Utopia or dystopia?

As we noted at the beginning of the story, with around 6 million CCTV cameras — or one

camera per 10 citizens — the UK has been called the world's most surveilled state. Earlier in the year, British police also started wearing body cameras, which are very effective at collecting evidence in call outs and public order incidents. Couple this with its existing database of criminal mugshots, and some judicious scanning of public Facebook profiles (which link your face to your name), and you can see how the police now have a *lot* of facial data to work with.

Andy Ramsay, one of the UK police officers using the NeoFace tech, said: "We have over ninety-thousand photos on our system and Neo-Face can compare someone's image against our complete databases in seconds. Besides the speed it's also impressive because it can even find family members related to the person we're trying to identify." Yes, if you look somewhat like your dad (i.e. you have the same nose or brow or lips) then NeoFace will probably throw up a potential match.



NEC's NeoFace Smart ID facial recognition companion app for smartphones and tablets

The obvious upside to facial recognition tech is that it's becoming increasingly hard to be a criminal. With 6 million CCTV cameras in the UK, there's a really good chance that you'll get spotted trying to mug someone or break into a house — and then you're just a few seconds away from being automatically identified by some software.

An error occurred.

Unable to execute Javascript.

The downside, of course, is that any expectation of privacy is quickly evaporating. The standard refrain from governments, intelligence agencies, and the police, of course, is that good people have nothing to hide — but it's really not that simple. With CCTV and facial recognition and license plate readers and NSA wire taps and even wearable computers like Google Glass, the concept of privacy is being rapidly eviscerated from our lives.

When we know that we're being watched and judged, we behave differently — *we conform*. Governments love this, of course — a docile population is an easy-to-rule population. But it's not even conformity that most scares me — it's the terrifying thought of what happens if these mass tools of surveillance are controlled by nefarious actors. In the hands of a good police, surveillance is a great way of reducing crime — but in the hands of an oppressive government or megacorporation, omnipresent surveillance is how society becomes dystopic, just like 1984.

FACIAL RECOGNITION AND IDENTIFICATION INITIATIVES

RICHARD W. VORDER BRUEGGE
FEDERAL BUREAU OF INVESTIGATION

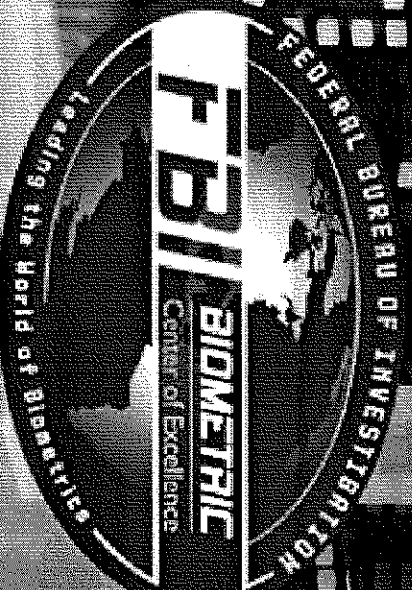
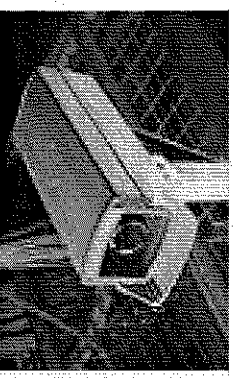
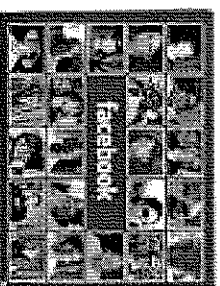
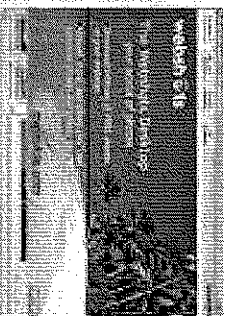
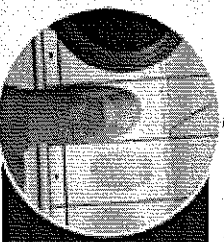


Image Technology in the Forefront

- Unparalleled ease of capturing, storing, copying, and sharing images
- Proliferation of surveillance cameras, expanding global media enterprises, and average citizens with mobile phone still and video camera capabilities
- Unprecedented level of sharing images and videos via the internet and other advanced communication methods
- Photographs and videos depicting victims, suspects, and eyewitnesses are becoming the subject of investigations

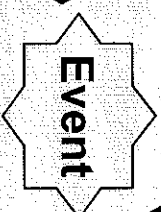


Face: Forensic Discipline And Biometric

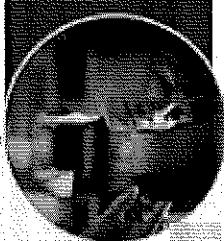


Biometrics

- A measurable biological (anatomical and physiological) or behavioral characteristic used for identification
 - Facial Recognition (FR) - the **automated** searching of a facial image in a computer database, typically resulting in a group of facial images ranked by computer-evaluated similarity



Forensics

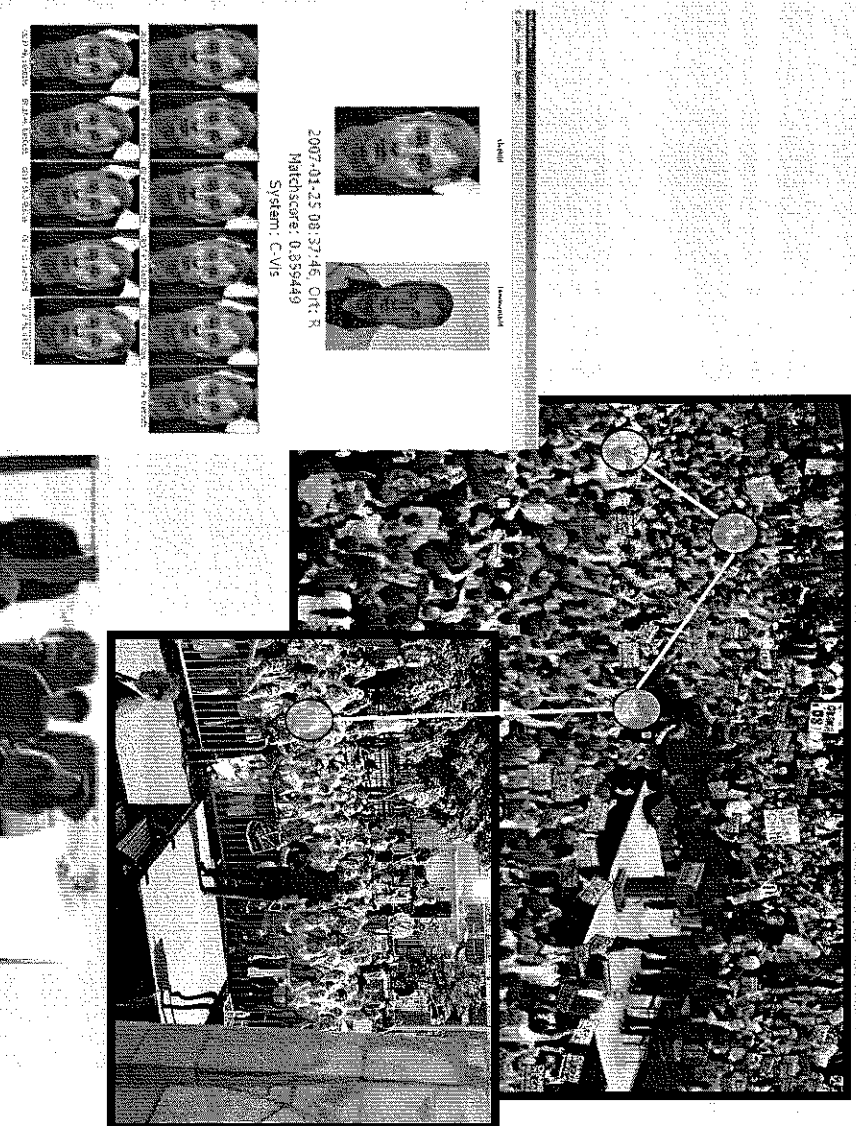


- Visible physical characteristics one can use for the purposes of measurements or comparisons that are collected after an event
 - Facial Identification (FI) - the **manual** examination of the differences and similarities between two facial images for the purpose of determining if they represent different persons or the same person



FI & FR Address Multiple Missions

- Mission Areas:
 - Access control
 - Automated identity verification
 - Human identification
 - Screening
 - Surveillance
 - Law enforcement & national security investigations
 - Identity intelligence to understand intent



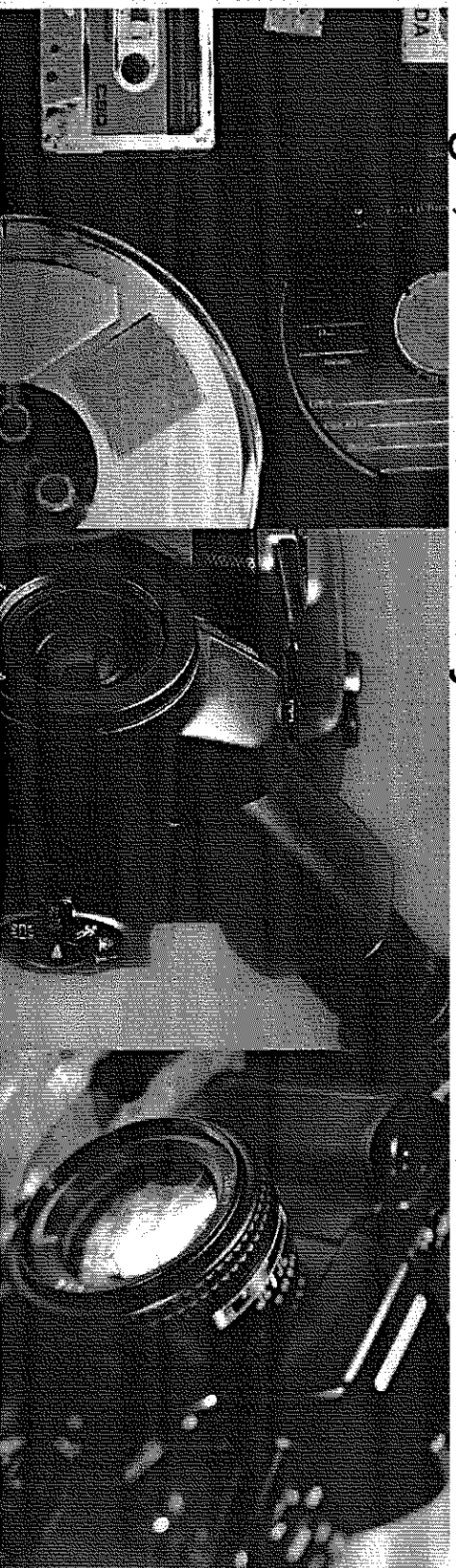
FBI Facial Use Cases

- Identifying fugitives and missing persons in FR systems
- Identifying unknown persons of interest from images (1:N)
- Tracking subjects movements to/from critical events (e.g., 9/11)
- Conducting automated surveillance at lookout locations (1:M, where $1 < M < N$)
- Identifying subjects in public datasets
- Identifying subjects from images in seized systems
- Verifying mug shots against National Criminal Information Center (NCIC) records (1:1)
- Controlling access

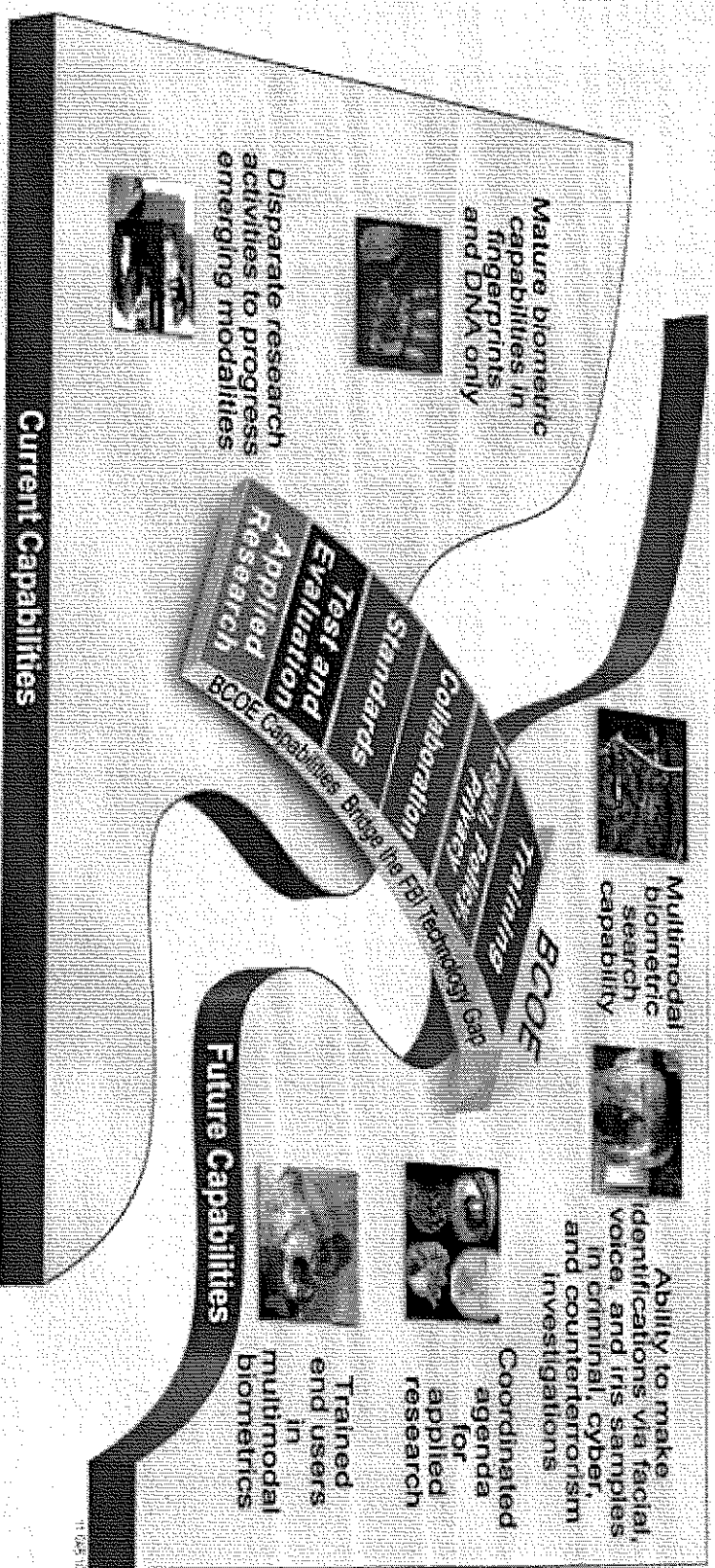


Identifying Subjects from Images for 40 Years

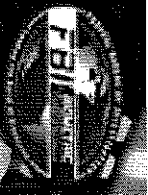
- The FBI's Facial Recognition/Identification work is performed within the Forensic Audio, Video, and Image Analysis Unit (FAVIAU)
- The FAVIAU is one of only a few accredited laboratories in the world that conducts examinations in the disciplines of video, image, and audio analysis



Driving New FBI Biometric Capabilities



The Biometric Center of Excellence (BCOE) is the Federal Bureau of Investigation's (FBI) program for exploring and advancing the use of new and enhanced biometric technologies and capabilities for integration into operations



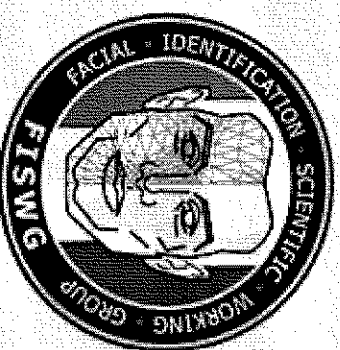
Sponsoring Applied Research

- Ongoing applied research, development, test & evaluation:
 - Universal Face & Iris Workstation
 - FBI Facial Collaboration-Facial Landmarking/Facial Aging
 - Automated Face Detection and Recognition in Video
 - FI/FR of Twins (blemishes)
 - Obscuring Identity in Video
 - ReproFace (2D-3D-2D)
 - Facial Image and Camera Certification Process
 - Automated Retrieval of Scars, Marks, and Tattoos
 - Ear Recognition
 - Multiple Biometric Grand Challenge/Multiple Biometric Evaluation/ III Data Set Testing



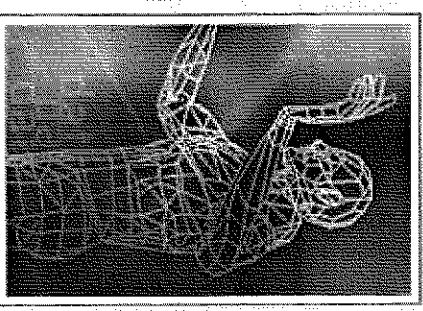
Sponsoring Standards Development

- Facial Identification Scientific Working Group (FISWG)
- Sponsored by the BCOE and established in 2009
- Mission - “develop consensus standards, guidelines, and best practices for the discipline of image-based comparisons of human features”
- Participants include federal, state, local, and international government agencies, as well as invited non-governmental organizations
- Next meeting scheduled for November 15-18 in San Antonio, Texas
- Visit www.FISWG.org



Deepening FR Collaboration

- Sponsored the International Face Collaboration Meeting
 - 5 foreign countries and 11 U.S. agencies participated
- Participated in the FR workshop “From Bones to Bits”
 - 55 U.S. government and 47 contractor attendees
- Sponsored the U.S. Government Facial Collaboration Meeting
 - 88 attendees representing numerous law enforcement, intelligence, and military agencies



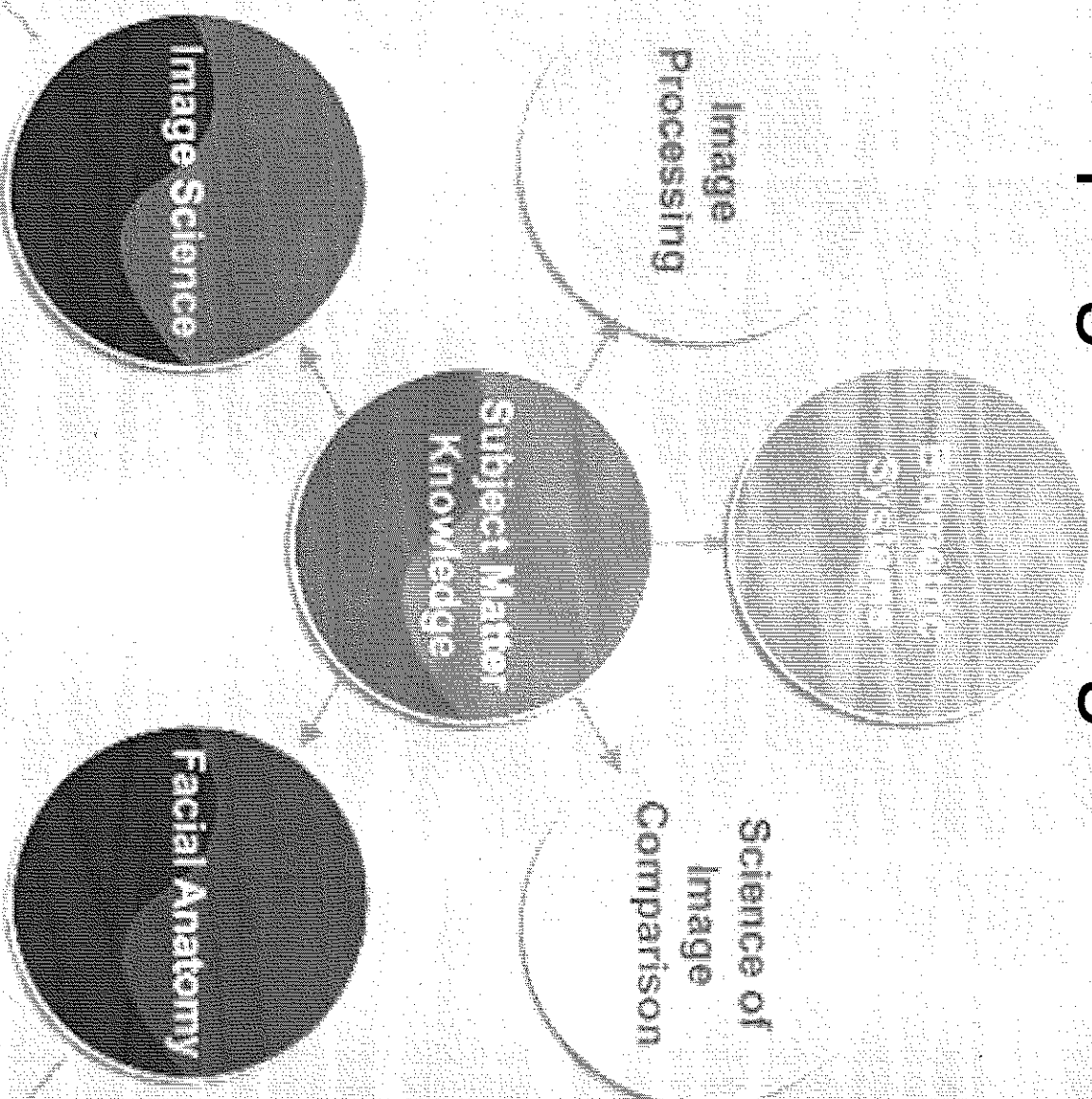
Analyzing Legal And Privacy Concerns

Tasks associated with this analysis include:

- Identifying databases external to the FBI to which the FBI has legal access
- Defining policy for both automated and human-tandem searching of databases and methods of how the images are used in searching and how they are destroyed or retained
- Identifying privacy implications of applied research using images of human subjects

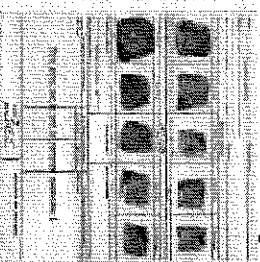
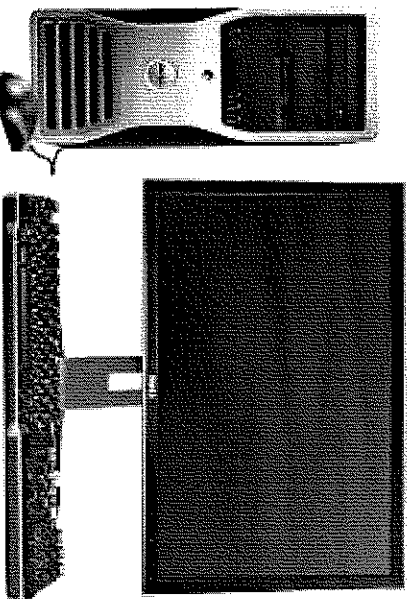


Developing Training Curriculum



Preparing for FR incorporation into Next Generation Identification (NGI)

- ▶ An upgrade to IAFIS – The FBI is developing an automated, interoperable multimodal biometric system



Enhanced
tenprint
services
2011



Palmprints
and latents
2012



Photos/Facial,
scars, marks,
and tattoos
2013



Iris
2014

- The NGI system:
 - Incremental replacement of the current IAFIS
 - Improving current functionality and providing new functionality
 - Developing multimodal collection and search identification services



Value Of the FBI-DMV Pilot

Operational Results

The BCOE-sponsored FR pilot program with NC DMV led to more than 700 leads including:

- One federal fugitive apprehension
- Six state fugitive apprehensions
- One missing person resolution

FR System Testing

FACEMASK has also served as an opportunity for FBI analysts to operationally test a FR system and determine its strengths and weaknesses. This aids the FBI as it develops its own FR capability

Identification of Follow-On Projects

Due to this success, the FBI took advantage of an ongoing survey of U.S. DMVs and used it as an opportunity to identify other prospective state DMVs for follow-on projects



Purpose Of The DMV Survey

The FBI wanted to identify key FR POC in order to direct inquiring investigators and agencies. The original DMV survey focuses around contact information; however, with the success of the original pilot the purpose and scope of the data gathering effort changed.

Initial Purpose

- Collect DMV FR POC Information
- Identify DMVs that have implemented FR systems

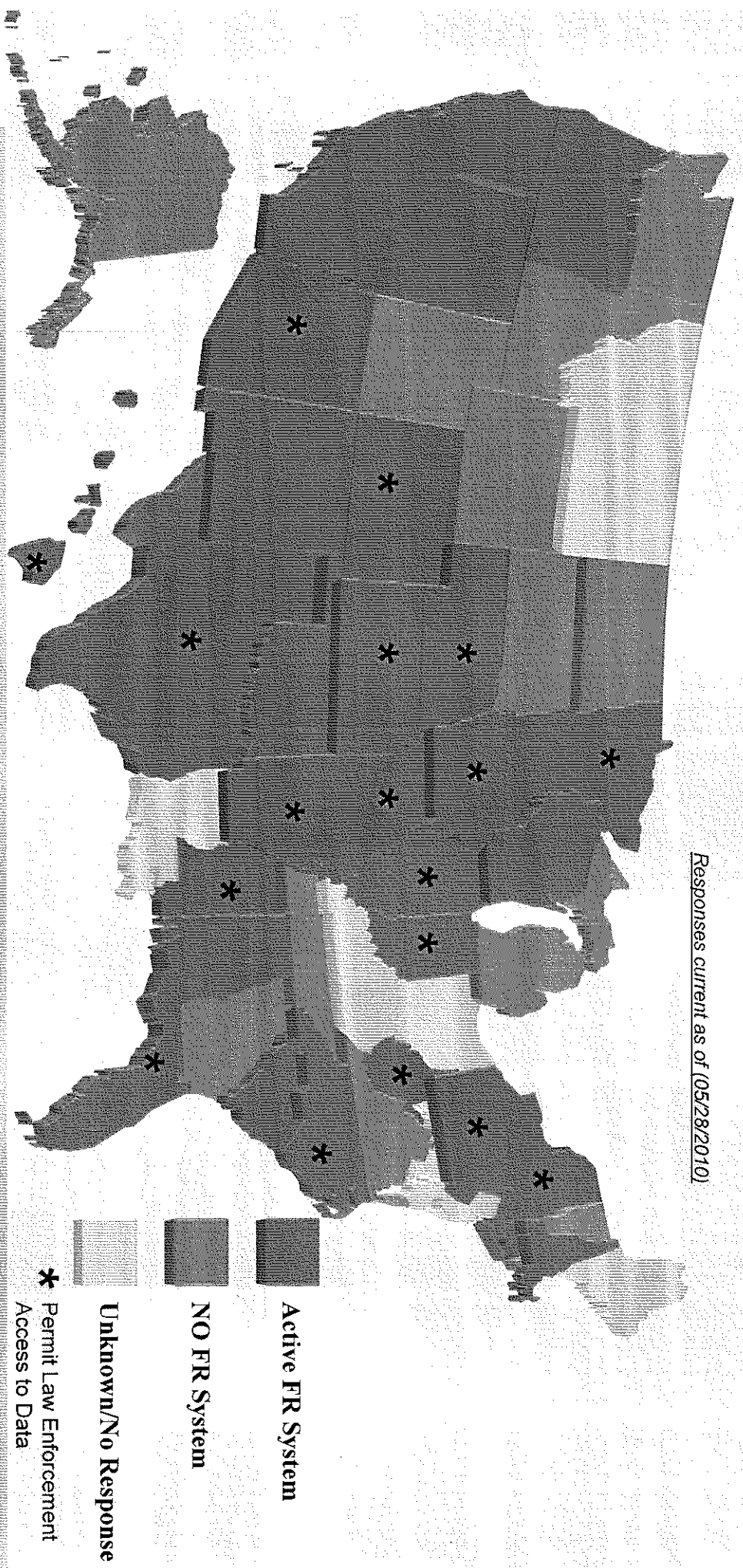
Expanded Purpose

- Gather data about FR vendors, state laws, and search protocol to help the FBI identify a DMV for a potential follow-on project
- Technical systems information
- Receptiveness to collaborating with the FBI
- Various concerns and suggestions voiced by the DMVs and trends were recorded



Potential FBI-DMV FR Pilot Expansion

Responses current as of (05/28/2010)



Key Takeaway: More than half of all state DMVs have FR systems. Their main goal is to detect and combat fraud



DMV Survey High Level Findings

Specific Findings

Technology

- ✓ The vast majority of states that have FR Systems use L1 Technologies

Vendors

- ✓ Many DMV image databases are maintained and searched by their vendors. This presents privacy issues that should be explored

Legal Requirements

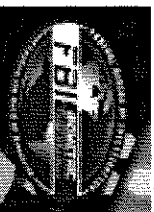
- ✓ Across the nation, there are widely varying legal requirements. To initiate searches, some DMVs require Memorandums of Understanding (MOU) while some just require the requesting agency to buy their vendor's software

Funding

- ✓ Due to a lack of funding, some states who had planned to develop FR systems had to delay or cancel their plans due to budgetary constraints

Knowledge

- ✓ Many DMV POCs lacked technical knowledge about their systems and the legal issues involved in their use. Since most POCs were unable or unwilling to nominate alternative POCs, more in-depth research may be required before FBI collaboration can be considered (i.e., researching state laws that apply to the DMV's FR system or interviewing a DMV's vendor for more specific systems information)



Questions / Comments

Contact Information:

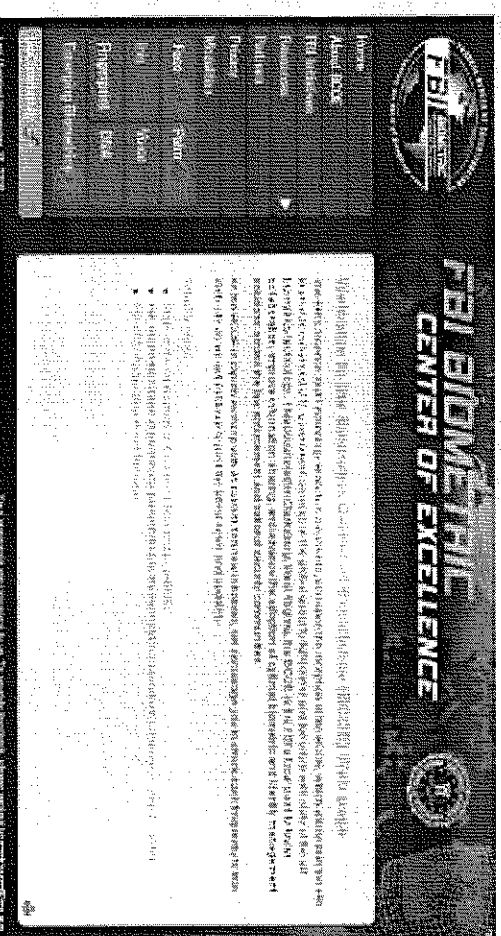
Richard Vorder Bruegge

Email: Richard.VorderBruegge@ic.fbi.gov

Additional Resources:

www.BiometricCoE.gov

Email: BiometricCoE@leo.gov



California cops sign contract to begin using massive biometric database

Published time: January 13, 2015 20:40

[Get short URL](#)

Reuters/Shannon Stapleton

[Facebook](#)[Twitter](#)[Reddit](#)[StumbleUpon](#)[Google+](#)[Tumblr](#)

Tags

Biology, Crime, Information
Technology, Intelligence, Police, SciTech, Social
networks, USA

The Los Angeles County Sheriff's Department – the fourth largest local policing agency in the United States – has taken another step towards building the biggest biometric database outside of the FBI's by inking a new \$24 million contract.

NEC Corporation of America – a Texas-based IT firm that provides biometric services to commercial entities, law enforcement groups, and governments around the globe – announced on Monday that it's been awarded a multi-year contract by the Los Angeles County Sheriff's Department to provide the agency with specialized, state-of-the-art policing services, including high-tech facial recognition software.

Previously published paperwork out of the LA County Board of Supervisors reveals that the Sheriff's Department requested approval last year for a \$24.4 million contract with NEC that would provide the agency – the largest sheriff's department in the US – with biometric

According to a statement put up by NEC Corp. this week, the deal will allow the LA Sheriff's Department to access fingerprint, palmprint, face, voice, iris and DNA matching capabilities offered through the company's Integra ID 5 Multimodal Biometrics Identification Solution (MBIS), as well as the NeoFace program touted by NEC being the "most accurate facial matching product" available in the world.

READ MORE: [FBI's facial recognition program hits 'full operational capability'](#)

Raffie Beroukhim, vice president of the NEC Biometrics Solutions Division, added in a statement that the company's products "will enable LASD to solve even more crimes and serve the public safety and security needs of citizens of Los Angeles County for years to come."

According to NEC, the biometric service being leased to Los Angeles law enforcement interfaces with databases maintained by outside agencies, including state, city and federal police groups such as the California Department of Justice, the Western Identification Network and the Next Generation Identity (NGI) – a system that the FBI elevated to operational status last September, allowing cops in Southern California to quickly, in theory, ID a suspect caught on closed-circuit surveillance cameras with any millions of images on any linked repository.

Lt. Thai, the Sheriff's Department employee tasked with implementing MBIS for LA County, told The Epoch Times last year that law enforcement officers won't collect biometric data on innocent Los Angelenos, but rather on individuals that have been arrested and booked in county jail or any of downtown LA's holding centers. Criminal charges don't always lend to successful convictions, however, meaning potentially millions of records pertaining to non-criminal Californians stand to end up in the database and thus at the disposal of the nation's largest sheriff's department.

READ MORE: FBI begins installation of \$1 billion face recognition system across America

As RT reported previously, the FBI's NGI system has been built up at a cost of \$1 billion over the last several years, with the goal of letting federal investigators easily access a database containing over 100 million individual records that may ink a person's biometric data – like individualized fingerprints and face scans – with personal information including home addresses, age and legal status. Allegations concerning an absence of oversight and proper privacy protections have alarmed digital rights advocates, however, and DC-based watchdog the Electronic Privacy Information Center previously sued the FBI in hopes of having the bureau disclose as much information as possible about the still infant system.

"The NGI database will include photographic images of millions of

individuals who are neither criminals nor suspects," attorney for EPIC

individuals who are neither criminals nor suspects, attorneys for EPIC previously argued in legal motions.

READ MORE: FBI sued over secretive mass surveillance program

And although the FBI recently announced that its massive NGL system is finally off the ground after years of development, the latest program to emerge out of Los Angeles will only amplify its scope by linking the details contained within both of those databases, among others.

Once completed, County officials intend on holding information on upwards of 15 million subjects within the Sheriff's Department database, *"giving the department a major stake in the Next Generation Identification program,"* according to the Center's report.

News concerning the LASD's contract with NEC was announced less than a week after the Texas firm confirmed that law enforcement agencies in two nearby counties – San Bernardino and Riverside – had entered into similar biometric contracts with the company. Two months earlier, NEC announced that its Integra-ID5 MBIS platform was being leased as a service model to the Western Identification Network, allowing eight states – including Alaska, Oregon, Nevada, and Montana – to take advantage of the system.

NEC claims its NeoFace facial recognition technology received the highest performance evaluation possible when reviewed by the US National Institute of Standards and Technology in 2013 and, by the firm's own admission, is successful 95 percent of the time at identifying individuals out of a pool of 1.8 million suspects.

Keith Raderschadt, NeoFace account manager for the Biometrics Solutions division of NEC Corporation, previously told Malaysia's The Star that the software can create 3D models of faces using only still images captured by CCTV cameras, and said the company's systems have already been adopted by the likes of the New York and Chicago Police Departments.

READ MORE: Chicago police start using facial-recognition software to arrest suspects

The Hong Kong office for NEC has previously suggested that its facial recognition technology may *"hold the key to facing the challenges of maintaining public order."* Meanwhile, its Tokyo branch was slated to show attendees at the 82nd ICPO-INTERPOL General Assembly Exhibition in Colombia how facial images, surveillance video footage and other *"physical sensor networks"* could be combined with *"cyber information surveillance"* obtained by monitoring Facebook accounts, blogs, message boards and chat rooms in order *"to identify the true source of an attack and physically locate a cyber-criminal."*

For now, though, LA County law enforcement is expected to implement their new biometric system without using it in concert with social media surveillance.

"It could be somebody gets pulled over for a traffic violation and he or she does not have a driver's license on him or her, and the officer is just trying to identify this person," Lt. Thai said last year to a local NBC News affiliate in explaining the positive benefits of the system.

As NBC acknowledged at the time, however, any data being stored in such a system will, for now, stay there for longer than the length of just a routine traffic stop. According to that report, biometric information collected by the FBI on a person without a criminal record will be purged when he or she turns 75.

Villarreal, Monique

From: Joseph, Paul
Sent: Tuesday, June 26, 2018 2:43 PM
To: Villarreal, Monique
Subject: Fw: FR Tech

From: Joseph, Paul
Sent: Tuesday, November 7, 2017 4:16 PM
To: Messier, Paul
Subject: Re: FR Tech

Perfect, thanks!

From: Messier, Paul
Sent: Tuesday, November 7, 2017 3:29:22 PM
To: Joseph, Paul
Subject: FR Tech

Lt. Paul Messier #3049

San Jose Police Department
Office of the Chief
Special Investigations Unit
408-537-1447 (Work)
[REDACTED] (Cell)

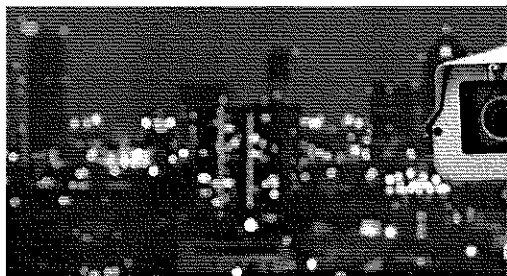
Villarreal, Monique

From: Joseph, Paul
Sent: Tuesday, June 26, 2018 2:43 PM
To: Villarreal, Monique
Subject: Fw: Facial Recognition

From: Todd Pastorini <TPastorini@DATAWORKSPLUS.com>
Sent: Monday, December 11, 2017 6:49 AM
To: Joseph, Paul
Subject: RE: Facial Recognition

Passing this along to all my agencies considering a Facial Recognition and street based camera system.

<https://resources.genetec.com/blog/how-the-city-of-detroit-reduced-violent-crime-by-50>



How the City of Detroit reduced crime by 50% - Genetec Inc.

resources.genetec.com

How Detroit's Police Department is using technology to improve safety across the Motor City

From: Todd Pastorini
Sent: Thursday, October 26, 2017 4:26 PM
To: 'paul.joseph@sanjoseca.gov' <paul.joseph@sanjoseca.gov>
Subject: Facial Recognition

Let me know if you need anything else.

Sincerely,
Todd Pastorini
Executive Vice President & General Manager
DataWorks Plus
(925)240-9010

•Mugshot Management • LiveScan Plus™ • Digital CrimeScene™ • Mobile Identification • Facial Recognition • Video Management

Villarreal, Monique

From: Joseph, Paul
Sent: Tuesday, June 26, 2018 2:44 PM
To: Villarreal, Monique
Subject: Fw: 10 Minutes

From: Schroder, Edward
Sent: Friday, January 26, 2018 11:30 AM
To: Joseph, Paul
Subject: Fw: 10 Minutes

From: Williams, Shawny
Sent: Thursday, January 25, 2018 3:21 PM
To: Schroder, Edward
Cc: Tindall, David
Subject: FW: 10 Minutes

<https://www.veritone.com/solutions/government/>

Government - Veritone, Inc.

www.veritone.com

Employ fully integrated, best-of-breed cognitive engines and potent applications acting in concert to transform and analyze media across content silos, delivering ...

We will need to setup a demonstration or presentation of this AI system and the NEC system that PJ talked with us about.

I don't know what this vendor's Facial Recognition capabilities are. Whatever demonstrations we plan, Judi, Fiscal, and some of our lieutenants should be included.

Let's try and schedule some demonstrations within two weeks. Please coordinate our schedules with Norma.

Shawny K. Williams

Deputy Chief of Police
Bureau of Investigations
San Jose Police Department

201 W. Mission St. San Jose, CA 95110
Office (408) 277-4002 Fax (408)298-8302
shawny.williams@sanjoseca.gov

From: Williams, Shawny
Sent: Thursday, January 25, 2018 2:59 PM
To: Schroder, Edward <EDWARD.SCHRODER@sanjoseca.gov>
Subject: FW: 10 Minutes

Ed,

Can you call this guy today.

Shawny K. Williams
Deputy Chief of Police
Bureau of Investigations
San Jose Police Department

201 W. Mission St. San Jose, CA 95110
Office (408) 277-4002 Fax (408)298-8302
shawny.williams@sanjoseca.gov

From: Garcia, Edgardo
Sent: Tuesday, January 23, 2018 5:03 PM
To: Williams, Shawny <SHAWNY.WILLIAMS@sanjoseca.gov>
Subject: FW: 10 Minutes

Shawny, can you vet this out. If you approve, maybe a staff presentation. I'm very interested, as I know you are, but its gotta be the right one...

EG

Edgardo Garcia
Chief of Police
San Jose Police Department
201 W. Mission St. 95110

Office (408) 277-4212

Cell [REDACTED]

From: Randa Akeel [<mailto:rakeel@veritone.com>]

Sent: Tuesday, January 23, 2018 8:01 AM

To: Garcia, Edgardo <EDGARDO.GARCIA@sanjoseca.gov>

Subject: 10 Minutes

Hi Edgardo,

I hope you are well. Just circling back on my last note regarding accelerated suspect identification using facial recognition technology.

When are you available for a brief call to discuss how Veritone uses artificial intelligence to enhance your investigations?

For more information, please refer to our [recent whitepaper](#) pertaining to known offender-related cases and digital evidence analysis.

Best Regards,

Randa Akeel

Business Development

(949) 335-6379 - ext 282 Direct

rakeel@veritone.com



Veritone 575 Anton Blvd Suite 900 Costa Mesa CA 92626

You received this email because you are subscribed to Marketing from Veritone.

Update your [email preferences](#) to choose the types of emails you receive.

[Unsubscribe from all future emails](#)

Villarreal, Monique

From: Joseph, Paul
Sent: Tuesday, June 26, 2018 2:45 PM
To: Villarreal, Monique
Subject: Fw: E-introduction

From: Joseph, Paul
Sent: Thursday, February 22, 2018 11:21 AM
To: Tindall, David
Subject: Re: E-introduction

The email does not include a phone number for these guys, so I sent them an email asking them to call me.

From: Tindall, David
Sent: Thursday, February 22, 2018 8:59:00 AM
To: Joseph, Paul
Subject: Re: E-introduction

Thanks Paul

Captain David Tindall
Commander/Bureau of Investigations
David.Tindall@sanjoseca.gov

San Jose Police Department
201 W. Mission Street
San Jose, CA 95110
(408)537-1500

From: Joseph, Paul
Sent: Thursday, February 22, 2018 8:55:30 AM
To: Tindall, David
Subject: Re: E-introduction

I will call the guy today.

From: Tindall, David
Sent: Wednesday, February 21, 2018 8:44:02 AM
To: Joseph, Paul
Subject: Fw: E-introduction

PJ,

From Schroeder

Captain David Tindall
Commander/Bureau of Investigations
David.Tindall@sanjoseca.gov

San Jose Police Department
201 W. Mission Street
San Jose, CA 95110
(408)537-1500

From: Schroder, Edward
Sent: Wednesday, February 21, 2018 8:30 AM
To: Tindall, David
Subject: Fwd: E-introduction

Dave, give this to Paul Joseph. He has been working on this and already has several vendors which he is in the process of lining up.

Sent via the Samsung Galaxy S® 6, an AT&T 4G LTE smartphone

----- Original message -----

From: "Williams, Shawny" <SHAWNY.WILLIAMS@sanjoseca.gov>
Date: 2/20/18 8:34 PM (GMT-08:00)
To: "Tindall, David" <DAVID.TINDALL@sanjoseca.gov>, "Schroder, Edward" <EDWARD.SCHRODER@sanjoseca.gov>
Subject: Fwd: E-introduction

Dave,

Can you work on this for the Chief since Schroder is out this week.

Thank you

Begin forwarded message:

From: "Williams, Shawny" <SHAWNY.WILLIAMS@sanjoseca.gov>
Date: February 16, 2018 at 11:38:38 AM PST
To: "Garcia, Edgardo" <EDGARDO.GARCIA@sanjoseca.gov>
Cc: "Knopf, Dave" <CHRISTOPHER.KNOPF@sanjoseca.gov>, "Tindall, David"

<DAVID.TINDALL@sanjoseca.gov>, "Schroder, Edward" <EDWARD.SCHRODER@sanjoseca.gov>

Subject: RE: E-introduction

Yes,

I will work on it today.

Shawny K. Williams
Deputy Chief of Police
Bureau of Investigations
San Jose Police Department

201 W. Mission St. San Jose, CA 95110
Office (408) 277-4002 Fax (408)298-8302
shawny.williams@sanjoseca.gov

From: Garcia, Edgardo
Sent: Friday, February 16, 2018 11:37 AM
To: Williams, Shawny <SHAWNY.WILLIAMS@sanjoseca.gov>
Cc: Knopf, Dave <CHRISTOPHER.KNOPF@sanjoseca.gov>; Tindall, David <DAVID.TINDALL@sanjoseca.gov>
Subject: FW: E-introduction

Shawny,

Can you coordinate for a staff meeting presentation?

Thx !!

Edgardo Garcia
Chief of Police
San Jose Police Department
201 W. Mission St. 95110
Office (408) 277-4212
Cell [REDACTED]

From: Sandoval Guerrero, Lilia
Sent: Friday, February 16, 2018 11:23 AM
To: Garcia, Edgardo <EDGARDO.GARCIA@sanjoseca.gov>
Cc: Peralez, Raul <Raul.Peralez@sanjoseca.gov>; john.chen@camvitech.com; Matt McCrann

<matt.mccrann@camvitech.com>

Subject: E-introduction

Good morning Chief Garcia,

Councilmember Perez would like to introduce you to John Chen, CC'd, president of Camvi Technologies Inc., a local company with a facial recognition technology that the Department might be interested, especially prior to updating the rest of our City's street light technology. Please consider meeting to further discuss this technology with Mr. Chen and Matt McCrann, CC'd, Camvi Technologies Inc.'s Director of Sales and Business Development. Thank you.

Best,

Lilia Sandoval Guerrero
Council Assistant
Office of Councilmember Raul Perez
City of San Jose, District 3
200 E. Santa Clara St., 18th Floor
San José, CA 95113
(408) 535-4928

Villarreal, Monique

From: Joseph, Paul
Sent: Tuesday, June 26, 2018 2:46 PM
To: Villarreal, Monique
Subject: Fw: Veritone AI Demo

From: Randa Akeel <rakeel@veritone.com>
Sent: Thursday, February 22, 2018 4:55 PM
To: Joseph, Paul
Subject: Re: Veritone AI Demo

Randa Akeel
Government Solutions
(949) 335-6379 ext. 282 direct
rakeel@veritone.com



Veritone, Inc.
575 Anton Blvd. Suite 900, Costa Mesa, CA. 92626
www.veritone.com

On Thu, Feb 22, 2018 at 4:48 PM, Randa Akeel <rakeel@veritone.com> wrote:
Hi Lt. Joseph,

Thank you for taking the time to speak with me today regarding Veritone's artificial intelligence capabilities to enhance investigations.

For more information, please refer to our [recent whitepaper](#) pertaining to known offender-related cases and digital evidence analysis as well as a [video](#) of our platform in action.

I look forward to hearing from you soon with possible dates for an on-site demonstration for the Chief and his command staff. Please let me know if you have any additional questions in the meantime.

Thank you again and have a wonderful day!

Best Regards,
Randa Akeel
Government Solutions
(949) 335-6379 ext. 282 direct
rakeel@veritone.com



Veritone, Inc.

575 Anton Blvd. Suite 900, Costa Mesa, CA. 92626

www.veritone.com

Villarreal, Monique

From: Joseph, Paul
Sent: Tuesday, June 26, 2018 2:47 PM
To: Villarreal, Monique
Subject: Fw: SJPDP - Camvi Technologies

From: Joseph, Paul
Sent: Tuesday, March 6, 2018 11:38 AM
To: Matt McCrann
Subject: Re: SJPDP - Camvi Technologies

The address for San Jose Police Department is 201 West Mission Street San Jose CA 95110. When you arrive, let the officer at the front desk know that you are here to see me. He will call upstairs to me, and I will bring you in.

Look forward to seeing you on Thursday 3-08-18 at 11:30.

From: Matt McCrann <matt.mccrann@camvitech.com>
Sent: Monday, March 5, 2018 9:41:26 AM
To: Joseph, Paul
Subject: SJPDP - Camvi Technologies

Hi Paul,

I'll be in San Jose this week for other meetings. I wanted to send you the latest capabilities brief for Camvi and see if there's anything we can do for you at this time to support your Unit's facial recognition needs and evaluation. I'm available to meet this week if you'd like to discuss or have any questions on the technology or how your unit can best use it in the field.

Here to help, however we can. Let me know!

Best regards,

Matt McCrann
Director, Sales & Business Development
Camvi Technologies
+1 202.468.8467

Villarreal, Monique

From: Joseph, Paul
Sent: Tuesday, June 26, 2018 2:48 PM
To: Villarreal, Monique
Subject: Fw: Facial Recognition software

From: Torrico, Judith
Sent: Thursday, March 15, 2018 9:16 AM
To: Joseph, Paul
Subject: RE: Facial Recognition software

Thanks, Paul, just trying to get an idea of the scope. I've read several articles and spoken to other agencies as there is a lot of legal issues that have to be dealt with. MugShot has higher match success rate due to picture quality – but will be interesting to see how they get it to match low light video, etc.

Looking forward to their demo.

Judi

From: Joseph, Paul
Sent: Thursday, March 15, 2018 8:57 AM
To: Torrico, Judith <Judith.Torrico@sanjoseca.gov>
Subject: Re: Facial Recognition software

So, any sort of technology is going to be controversial in the Bay Area, and facial recognition has been controversial wherever it has been used. Chief Garcia is very interested in acquiring some sort of limited capability, however, and I'm sure he can navigate the political waters.

What we are looking at is something that I think would be the least controversial possible application of this technology. We would like the capability to compare surveillance photos of suspects from in-progress crimes to photos from our mugshot database. Another possible application is the ability to take a photo of a person detained in the field and compare that photo to the mugshot database through a cell phone based app. We are NOT looking at placing fixed cameras at locations throughout the city and detaining people based on comparisons and potential matches!

As far as permission to access the mugshot database, there will not be an issue if we go with DataWorks. As you know, they already manage the mugshot photo database for SJPd and the S.O. DataWorks also is the exclusive distributor for NEC Corporation, which designed the "Neoface Program", the leading facial

recognition technology in the industry. I'm not sure if there would be legal issues with some other company accessing the DataWorks mugshot database. That is one of many questions that I'm sure we would turn to the City Attorney to answer.

I'm not sure where the funding for this is going to come from. As I mentioned, Chief Garcia is a big proponent. Possibly it will be a budget request he makes to City Council, it may come from some grant, or it may come from this proposed public safety bond measure that is being discussed.

Hopefully, that answers some of your questions. Again, we are in the very preliminary stages of trying to figure all of this out. Please feel free to contact me with any other questions.

From: Torrico, Judith
Sent: Thursday, March 15, 2018 7:55:32 AM
To: Joseph, Paul
Cc: Schroder, Edward
Subject: RE: Facial Recognition software

Hello Paul,

Thank you for reaching out and bringing me up to speed on the latest technology procurement. Agreed, IT staff should be present at these type of demos/presentations as to configuration, functionality, and ongoing IT support.

Paul, can you please provide a little more information as to what the Department is looking for with Facial Recognition? What is the proposed DB the recognition is going to compare to? MugShot DB? What permission do we need to get to use those photos from the S.O.? Do we have the funding for this project or is this going to be used to submit a budget proposal?

Schedules are very difficult – I will move a meeting, and both Rudy and I will be there for the demo.

Thanks,

Judi

From: Joseph, Paul
Sent: Wednesday, March 14, 2018 3:02 PM
To: Torrico, Judith <Judith.Torrico@sanjoseca.gov>
Cc: Schroder, Edward <EDWARD.SCHRODER@sanjoseca.gov>
Subject: Facial Recognition software

I have been tasked with doing preliminary research on the various companies that offer facial recognition technology. At this stage, I am setting up meetings with sales reps from several companies to see specifically what they have to offer. D.C. Williams, Captain Schroder, Captain Tindall, myself, and several other BOI Lieutenants attended the first meeting. We hope to do a preliminary vetting of the companies before deciding

which companies have a realistic chance of meeting our needs, and having them return for a presentation to Chief Garcia.

It was evident to me at the first meeting that it would be great to have you or someone from your staff attend any future meetings with the sales reps. The last presentation raised a number of issues that we were only somewhat prepared to understand. I'm sure you would have a number of questions that we would not even think of!

I have a meeting scheduled with the sales rep from DataWorks on Tuesday April 17 at 11:00 in the PCC. Getting a D.C. and two Captains in one place was no small endeavor! I also know that you have an extremely busy schedule. I apologize for not coordinating with you in advance. Regardless, I am hoping that you or someone from your staff would be able to attend.

Please let me know your availability.

PJ #3148

Villarreal, Monique

From: Joseph, Paul
Sent: Tuesday, June 26, 2018 2:49 PM
To: Villarreal, Monique
Subject: Fw: Face Id Training this March
Attachments: Facial Identification Flyer.pdf

From: Todd Pastorini <TPastorini@DATAWORKSPLUS.com>
Sent: Tuesday, April 17, 2018 3:37 PM
To: Joseph, Paul
Subject: FW: Face Id Training this March

Paul,

In the event that you are looking for training on FR and industry practices beyond what DataWorks Plus provides, I thought I would send you this.

Todd

From: Mark Dolfi [mailto:mark.dolfi@dataworksplus.com]
Sent: Monday, January 29, 2018 7:54 PM
Subject: Face Id Training

Hello,

This is Mark Dolfi, here is the email I spoke about where I developed a 16-hour Facial Identification Training Course, which a flyer is attached. This course is different from the 8-hour LA Photomanager class I teach at LACRIS as it fully meets the recommendations set by the Facial Identification Scientific Working Group (FISWG). This is a venture that I am seeking outside of the Sheriff's Department and has no affiliation to them.

It is rumored that the FBI will soon require any law enforcement official who requests a facial recognition search through their NGI FACE Services Unit, to possess at least a basic level of knowledge. They have identified that the basic level of knowledge requirements are very similar to what is found in FISWG's Guidelines and Recommendations for Facial Comparison Training to Competency document. The 40-hour class offered by a couple of vendors, although beneficial, can be hard to accomplish with your workload, tuition and travel arrangements. It is not possible to meet these requirements in an 8-hour class that focuses on a facial recognition system's functions. This is why my 16 hour class was developed. It meets those FBI requirements it seeks and I can travel to your agency.

As the current IAI Chair of the Facial Identification Subcommittee, our group is tasked with creating a training program that can be hopefully certified by the IAI in both a 16 (basic) and 40 (advanced) hour

level soon. The FBI works closely with FISWG and the IAI to share and create the guidelines, standards and best practices for facial identification and we look forward to accomplishing this task.

Take a look at the flyer and the website for more information on hosting a class at your agency. I do offer a class locally, however, they are on a small scale and do not run on a specific schedule. I plan to travel to agencies around the country in hopes of preparing everyone for the future of facial identification.

If you have any questions at all, you can reply to this email or use the contact us page on the website.

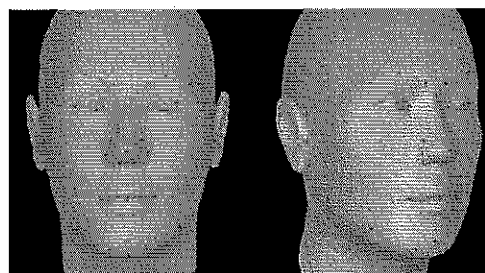
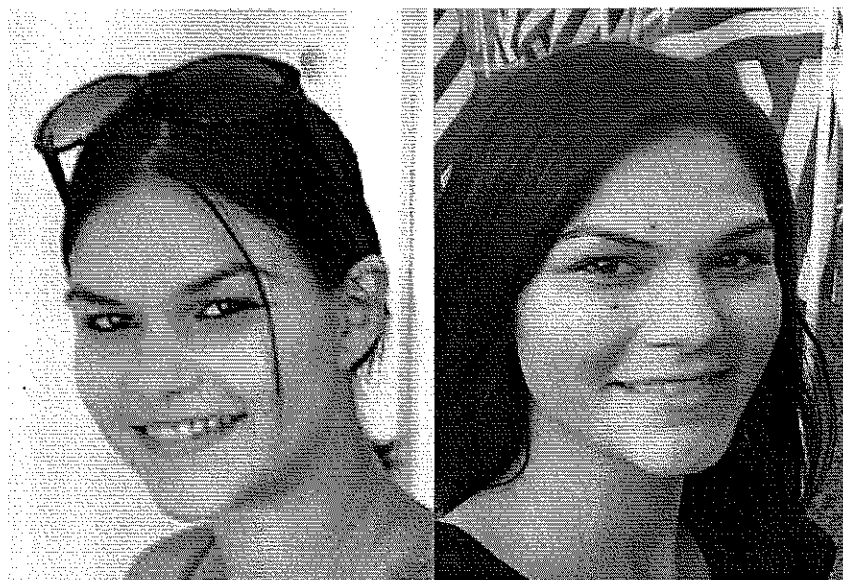
Looking forward to hearing from you!

Mark

In Your Face Id Training
714-576-7300

IN YOUR FACE ID TRAINING

ARE YOU READY
TO TESTIFY ABOUT FACIAL
IDENTIFICATION?



Sign up now for a 2-day facial identification course

March 26th & 27th 7:00am-3:30pm
Black Gold Golf Club, 1 Black Gold Dr., Yorba Linda, CA

This two-day course will introduce students to more than just the basics of facial identification or how a facial recognition system works. It will cover many aspects including the different approaches used every day by federal, state and local law enforcement agencies around the globe.

This course has been developed specifically for investigators, crime analysts, and fingerprint examiners. You will be comparing images from the get-go and be taught the techniques to pass the proficiency test at the end of the course.

Tuition starts at \$369 per student – Limited Seating!

Visit us at www.inyourfaceidtraining.com
or call 714-576-7300 for more information

Topics to be covered

*Facial identification
standards, guidelines &
recommendations*

*Courtroom Preparation &
Testimony*

*Facial recognition systems;
their algorithms & limitations*

*Sharing criminal
information*

Morphological Analysis

*Anatomy of the face,
head and neck*

...and much more

Villarreal, Monique

From: Joseph, Paul
Sent: Tuesday, June 26, 2018 2:50 PM
To: Villarreal, Monique
Subject: Fw: Contacts

From: Todd Pastorini <TPastorini@DATAWORKSPLUS.com>
Sent: Tuesday, April 17, 2018 3:42 PM
To: Joseph, Paul
Subject: Contacts

Mark Dolfi
Los Angeles County Sheriff's
mADolfi@lasd.org
[REDACTED]

Michael Thompson
mthompson@riversidesheriff.org
or
Stephanie Trott
strott@riversidesheriff.org
Riverside County Sheriff's Department
[REDACTED]

Jerry Harper, Systems Support Analyst II
San Bernardino County Sheriff/Coroner Department
Scientific Investigations Division
Biometric Identification Network (CAL-ID)
880 East Mill Street
San Bernardino, CA 92415-0054
(W): 909-890-5046
(F): 909-890-5045
[REDACTED]
jharper@sbcasd.org

FRANK SULLIVAN

*Automated Systems Analyst
San Bernardino County Sheriff's Department
Scientific Investigations Division - CAL-ID
880 East Mill St. San Bernardino, CA 92415
Email: fsullivan@sbcasd.org Desk: 909-890-5043*

Sincerely,

Todd Pastorini
Executive Vice President & General Manager
DataWorks *Plus*
(925)240-9010

• Mugshot Management • LiveScan Plus™ • Digital CrimeScene™ • Mobile Identification • Facial Recognition • Video Management

Villarreal, Monique

From: Joseph, Paul
Sent: Tuesday, June 26, 2018 2:50 PM
To: Villarreal, Monique
Subject: Fw: Remote Access Network
Attachments: CAL-ID - Agenda -3.13.2018.pdf

From: Schroder, Edward
Sent: Thursday, April 19, 2018 7:51 AM
To: Joseph, Paul
Subject: Fwd: Remote Access Network

Sent via the Samsung Galaxy S® 6, an AT&T 4G LTE smartphone

----- Original message -----

From: "Torrico, Judith" <Judith.Torrico@sanjoseca.gov>
Date: 4/19/18 7:48 AM (GMT-08:00)
To: "Joseph, Paul" <PAUL.JOSEPH@sanjoseca.gov>
Cc: "Williams, Shawny" <SHAWNY.WILLIAMS@sanjoseca.gov>, "Schroder, Edward" <EDWARD.SCHRODER@sanjoseca.gov>
Subject: RE: Remote Access Network

Good Morning Paul,

Yes, I am somewhat familiar with the Cal-ID/RAN Policy Board. Chief Garcia attended the recent annual meeting which was held on March 13, 2018. There are a total of six seats on the board:

BOARD MEMBERS:

- Chief Phan Ngo(Chair)
- Supervisor Mike Wasserman
- District Attorney Jeff Rosen
- Chief Eddie Garcia
- Sheriff Laurie Smith
- Mayor Gary Waldeck, Los Altos Hills

Unfortunately, I was not able to attend the meeting with the Chief as [REDACTED] Reviewing the 2017 meeting notes and SCCCCO Cal ID Program annual report, funds are specifically allocated this year to

Mugshot maintenance (Dataworks \$225,000) and several other technology projects. They also have an Approved Technology Plan Expense of \$2.4M which includes Mobile ID Program hardware and software (\$1,23M), Justice Systems Interoperability (\$300K), AFIR network upgrade (\$100K), disaster recovery (\$500K), technology refresh (\$250K). The funds are controlled by the Board & project appear to be regional in nature.

I will reach out to my counterpart at the Sheriff's Office to inquire as to how San Jose can request certain projects and or the process to submit projects for funding.

Thanks,

Judi



Judi Torrico
Deputy Director, Bureau of Technical Services
San José Police Department
855 N. San Pedro Street | San Jose, CA 95110
Tel: (408) 277-5176

CONFIDENTIALITY NOTICE: This communication with its contents may contain confidential and/or legally privileged information. This communication with its contents may contain confidential and/or legally privileged information. It is solely for the use of the intended recipient(s). Unauthorized interception, review, use or disclosure is prohibited and may violate applicable laws including the Electronic Communications Privacy Act. If you are not the intended recipient, please contact the sender and destroy all copies of this communication.

From: Joseph, Paul
Sent: Wednesday, April 18, 2018 4:01 PM
To: Torrico, Judith <Judith.Torrico@sanjoseca.gov>
Cc: Williams, Shawny <SHAWNY.WILLIAMS@sanjoseca.gov>; Schroder, Edward <EDWARD.SCHRODER@sanjoseca.gov>
Subject: Remote Access Network

Have you heard of the Remote Access Network (RAN)? I'm sure you have, but it is something I learned about today after talking to the facial recognition expert from the L.A. County Sheriff's Department.

Each county in California has a RAN Board that manages a RAN fund made up of money collected through court costs assessed to criminal defendants, and money collected for this specific purpose as part of DMV vehicle registration fees. The RAN is set up pursuant to Penal Code 11112.4. These RAN funds can be accessed for technology purposes related to the identification of criminal suspects, such as facial recognition technology. He told me it may be easier to access these funds than it is to get grant funds, and would not have all of the conditions tied to it that grant funds have.

Let me know if you are familiar with this. If not, I will continue looking into who manages this fund in Santa Clara County, how much money is in the fund, and how we might go about accessing some of the money. If you are familiar with it, let me know if you think this source of funding is worth pursuing.

Thanks for your help!

PJ #3148

**SANTA CLARA COUNTY
CAL-ID RAN POLICY BOARD**

TO: CAL-ID RAN POLICY BOARD

FROM: Phan Ngo, Chair/Police Chief, Sunnyvale
Department of Public Safety

SUBJECT: CAL-ID RAN Board Meeting

This is a notice that there will be a meeting of the Santa Clara County CAL-ID RAN Policy Board on:

Tuesday, March 13th, 2018, at 3:30 p.m.
Santa Clara County Office of the Sheriff
55 West Younger Avenue
4th Floor, Large Conference Room
San Jose, California 95110
(408) 808-4900

AGENDA:

1. Approve Minutes of March 7, 2017 Board Meeting
2. SIU Accreditation
3. Budget and Allocation Update
4. Technology Update
5. Approve SB 720 Budget and Technology Plan
6. Approve Annual Report

Villarreal, Monique

From: Joseph, Paul
Sent: Tuesday, June 26, 2018 2:51 PM
To: Villarreal, Monique
Subject: Fw: RAN Board

From: Dolfi, Mark A. <mADolfi@lasd.org>
Sent: Tuesday, May 8, 2018 6:04 AM
To: Joseph, Paul
Subject: RE: RAN Board

Sir,

If you're in the LA area on the 30th of May and want to learn more about the Data Works FR system, let me know.

I always hold 3-4 spots for late registration, so if it's last minute, not a problem.

Facial Recognition and the LA
PhotoManager Register

**Registration closes 24 hours prior to class
time**

Time: 07:00 AM - 03:30 PM
Date: 05/30/2018 - 05/30/2018
Only 13 Seats Remaining

My outside FR company will be at Sacramento Sheri'ff's on June 14-15 for a 2 day class but that's not 100% free like the LA one. ☺

Mark

Mark A. Dolfi
LACRIS - Data Systems Bureau
12440 E. Imperial Hwy, Ste 400W
Norwalk, CA 90650
[REDACTED] ph
323-415-1938 fx
madolfi@lasd.org

From: Joseph, Paul [<mailto:PAUL.JOSEPH@sanjoseca.gov>]
Sent: Wednesday, April 18, 2018 10:21 AM
To: Dolfi, Mark A. <mADolfi@lasd.org>
Subject: RAN Board

It was great learning from you about facial recognition technology.

Thanks for forwarding me the name of the RAN Board contact for Santa Clara County.

Lt. Paul Joseph #3148
San Jose Police Department
Bureau of Investigations/Robbery Unit

Villarreal, Monique

From: Joseph, Paul
Sent: Tuesday, June 26, 2018 2:52 PM
To: Villarreal, Monique
Subject: Fw: Presentation by Veritone

From: Randa Akeel <rakeel@veritone.com>
Sent: Tuesday, May 8, 2018 2:08 PM
To: Joseph, Paul
Subject: Re: Presentation by Veritone

I also just sent a new google calendar invitation. Please feel free to invite the others who will be attending.

Thank you again,
Randa Akeel
Business Development
(949) 335-6379 direct
rakeel@veritone.com



Veritone, Inc.
575 Anton Blvd. Suite 900, Costa Mesa, CA. 92626
www.veritone.com

On Tue, May 8, 2018 at 1:41 PM, Randa Akeel <rakeel@veritone.com> wrote:
Hi Lt. Joseph,

Yes, we are confirmed for Wednesday, May 30th at 1:00 pm.

My VP of Government Solutions, Tom Avery and Sr. Account Executive of Government Solutions, Jeff Reeve (cc'd on this email) will be presenting.

Thank you again and we look forward to meeting with you and your command staff.

All the best,
Randa Akeel
Business Development

(949) 335-6379 direct
rakeel@veritone.com



Veritone, Inc.

575 Anton Blvd. Suite 900, Costa Mesa, CA. 92626

www.veritone.com

On Tue, May 8, 2018 at 10:24 AM, Joseph, Paul <PAUL.JOSEPH@sanjoseca.gov> wrote:

I am confirming that we will meet with you or your representatives at the San Jose Police Department on Wednesday May 30th at 1:00 P.M.

Thank you, and we look forward to your presentation!

From: Randa Akeel <rakeel@veritone.com>

Sent: Thursday, May 3, 2018 11:30:38 AM

To: Joseph, Paul

Subject: Re: Presentation by Veritone

Hi Lt. Joseph,

I hope you are doing well! I wanted to follow up to see if your department is available to meet within the next month or two?

Thank you and looking forward to connecting again soon.

All the best,

Randa Akeel

Government Solutions

(949) 335-6379 direct

rakeel@veritone.com



Veritone, Inc.

575 Anton Blvd. Suite 900, Costa Mesa, CA. 92626

www.veritone.com

On Wed, Mar 14, 2018 at 3:15 PM, Joseph, Paul <PAUL.JOSEPH@sanjoseca.gov> wrote:

Thank you for agreeing to come to San Jose PD to do a presentation on what Veritone offers in the area of facial recognition technology.

The presentation will be on Tuesday April 24, 2018 at 1:00 PM. The presentation will be held at the San Jose Police Department 201 West Mission Street San Jose CA 95110 in the Police Command Center. Deputy Chief Shawny Williams, Captain Ed Schroder, Captain Dave Tindall, myself, and several other B.O.I. Lieutenants will attend.

When you arrive, please let the Officer at the front desk know that you are there to see me. I will come down to the lobby and walk you upstairs. If you need to cancel for any reason, please call me at 408-277-4166.

Lt. Paul Joseph #3148
San Jose Police Department
BOI/Robbery

Villarreal, Monique

From: Joseph, Paul
Sent: Tuesday, June 26, 2018 2:52 PM
To: Villarreal, Monique
Subject: Fw: Special Projects

From: Schroder, Edward
Sent: Wednesday, June 6, 2018 1:52 PM
To: Joseph, Paul
Subject: Re: Special Projects

Thank you Paul

From: Joseph, Paul
Sent: Wednesday, June 6, 2018 1:00:43 PM
To: Schroder, Edward
Subject: Special Projects

I have the following "special projects" working in the Robbery Unit:

1. Interview and Interrogation School. The Department has an ongoing contract with Reid and Associates to provide training to BOI on Interview and Interrogation. The next four day school is scheduled for October 2-5. The long term plan is to host such a class every 6 months in order to provide this training to all incoming Detectives in BOI as soon as possible upon their assignment to BOI.
2. BOI On Call. I coordinate the scheduling and operations of the BOI On Call program. The program ensures that two BOI Detectives, typically one Sergeant and one Officer, are available as a resource to Patrol 24/7. This is an ongoing program that shall continue until further notice.
3. Facial Recognition research. I have been involved in researching the acquisition of facial recognition technology for the SJPD. I have researched the companies providing such a service, and have brought three companies in for demonstrations of their products. I have also researched funding sources for the technology, which will cost approximately \$350,000. The status of this program is that we need to meet with Chief Garcia to recommend one of the three companies (Dataworks), schedule a demonstration for Chief Garcia, and finalize a source of funding for the technology.

PJ #3148

Villarreal, Monique

From: Joseph, Paul
Sent: Tuesday, June 26, 2018 2:53 PM
To: Villarreal, Monique
Subject: Fw: Jeff Reeve from Veritone

From: Jeff Reeve <jreeve@veritone.com>
Sent: Monday, June 18, 2018 8:56 AM
To: Joseph, Paul
Subject: Re: Jeff Reeve from Veritone

Thanks for getting back to me Lt. and letting me know. I hope it works out and if not, please feel free to let me know.

Thank You

Jeff Reeve
Sr. Account Executive Government Solutions
[REDACTED] mobile
(888) 507-1737 direct
jreeve@veritone.com



Veritone, Inc.
575 Anton Blvd. Suite 100, Costa Mesa, CA. 92626
www.veritone.com

On Jun 14, 2018, at 8:52 AM, Joseph, Paul <PAUL.JOSEPH@sanjoseca.gov> wrote:

Thank you very much for your recent presentation. After attending presentations from several vendors, we have decided to make a recommendation to Chief Garcia to pursue a relationship with another company.

From: Jeff Reeve <jreeve@veritone.com>
Sent: Friday, June 8, 2018 2:36:28 PM
To: Joseph, Paul
Subject: Jeff Reeve from Veritone

Lt.,

I wanted to reach out to you again to see if there is still any interest in a follow up with us or getting you the contact information you requested. Please let me know either way as I don't want to pester you if you have decided to go down a different path.

Thank You

Jeff Reeve

Sr. Account Executive Government Solutions

[REDACTED] mobile

(888) 507-1737 direct

jreeve@veritone.com



Veritone, Inc.

575 Anton Blvd. Suite 100, Costa Mesa, CA. 92626

www.veritone.com

Villarreal, Monique

From: Joseph, Paul
Sent: Tuesday, June 26, 2018 2:54 PM
To: Villarreal, Monique
Subject: Fw: Amazon F/R

From: Joseph, Paul
Sent: Friday, June 22, 2018 9:52 AM
To: Barreto, Joaquin
Subject: Re: Amazon F/R

Do you have a contact person at the company that I could call to see what they are actually proposing in a little more detail?

From: Barreto, Joaquin
Sent: Thursday, June 21, 2018 10:54:38 PM
To: Joseph, Paul
Subject: Amazon F/R

Hey Paul,

Here's the company offering to partner with PD to assist identifying suspects by using F/R and our database. It basically appears to be the same thing that Amazon is also doing for Washington County Sheriff. (see second link)

<https://www.smarthomesentry.com/>

<http://www.wweek.com/news/courts/2018/05/22/amazon-sold-powerful-facial-recognition-software-to-the-washington-county-sheriff-and-gresham-police/>

Hopefully make some of our job easier!

Villarreal, Monique

From: Joseph, Paul
Sent: Tuesday, June 26, 2018 2:55 PM
To: Villarreal, Monique
Subject: Fw: Presentation by DataWorks on Facial Recognition Software

From: Todd Pastorini <TPastorini@DATAWORKSPLUS.com>
Sent: Tuesday, June 26, 2018 9:21 AM
To: Joseph, Paul
Subject: RE: Presentation by DataWorks on Facial Recognition Software

Paul,

How did we do in the evaluation process? I would appreciate any feedback you have so that we may stay competitive in the market place.

Todd

From: Joseph, Paul [mailto:PAUL.JOSEPH@sanjoseca.gov]
Sent: Monday, May 21, 2018 9:10 AM
To: Todd Pastorini <TPastorini@DATAWORKSPLUS.com>
Subject: Re: Presentation by DataWorks on Facial Recognition Software

Thank you for the quote. We are going to meet with one more vendor next week. After that, we will make a recommendation to Chief Garcia as to which vendor we recommend. Then, we have to figure out how we are going to pay for it! That last part may take some time. I will keep you posted.

From: Todd Pastorini <TPastorini@DATAWORKSPLUS.com>
Sent: Sunday, May 20, 2018 8:25:10 AM
To: Joseph, Paul
Subject: RE: Presentation by DataWorks on Facial Recognition Software

Please disregard the last quote. There was some mathematical errors.

From: Todd Pastorini
Sent: Sunday, May 20, 2018 7:43 AM
To: 'Joseph, Paul' <PAUL.JOSEPH@sanjoseca.gov>
Subject: RE: Presentation by DataWorks on Facial Recognition Software

Lt. Joseph,

I am sorry for the lengthy delay on this proposal. I am still waiting on pricing from NEC, but I wanted to get this proposal in your hands. Let me know what the next step is.

Sincerely,
Todd Pastorini
Executive Vice President & General Manager
DataWorks *Plus*
(925)240-9010

• Mugshot Management • LiveScan Plus™ • Digital CrimeScene™ • Mobile Identification • Facial Recognition • Video Management

From: Joseph, Paul [<mailto:PAUL.JOSEPH@sanjoseca.gov>]
Sent: Monday, April 16, 2018 12:49 PM
To: Todd Pastorini <TPastorini@DATAWORKSPLUS.com>
Subject: RE: Presentation by DataWorks on Facial Recognition Software

Great, see you then!

Sent from the Samsung Galaxy Rugby Pro, an AT&T LTE smartphone

----- Original message -----

From: Todd Pastorini <TPastorini@DATAWORKSPLUS.com>
Date: 04/16/2018 11:39 (GMT-08:00)
To: "Joseph, Paul" <PAUL.JOSEPH@sanjoseca.gov>
Subject: RE: Presentation by DataWorks on Facial Recognition Software

Lt. I will try to be there by 10:45 tomorrow to allow time for setup.

Todd

From: Joseph, Paul [<mailto:PAUL.JOSEPH@sanjoseca.gov>]
Sent: Wednesday, March 14, 2018 4:26 PM
To: Todd Pastorini <TPastorini@DATAWORKSPLUS.com>
Subject: Re: Presentation by DataWorks on Facial Recognition Software

No problem. The room we will be in has all of that.

From: Todd Pastorini <TPastorini@DATAWORKSPLUS.com>
Sent: Wednesday, March 14, 2018 4:21:45 PM
To: Joseph, Paul
Subject: RE: Presentation by DataWorks on Facial Recognition Software

Paul,

I will have a laptop and will either need access to the internet or a room that I can get Verizon service in and use my phone as a hot spot. I can bring a projector.

Todd

From: Joseph, Paul [<mailto:PAUL.JOSEPH@sanjoseca.gov>]
Sent: Wednesday, March 14, 2018 2:46 PM
To: Todd Pastorini <TPastorini@DATAWORKSPLUS.com>
Cc: Williams, Shawny <SHAWNY.WILLIAMS@sanjoseca.gov>; Schroder, Edward <EDWARD.SCHRODER@sanjoseca.gov>; Tindall, David <DAVID.TINDALL@sanjoseca.gov>; Amaro, Norma A <Norma.Amaro@sanjoseca.gov>; Torrico, Judith <Judith.Torrico@sanjoseca.gov>
Subject: Presentation by DataWorks on Facial Recognition Software

Thank you for agreeing to come to San Jose PD to give a presentation on what DataWorks has to offer in the area of facial recognition technology.

The date for our meeting will be Tuesday April 17, 2018 at 11:00 A.M. We will hold the meeting in the Police Command Center at San Jose PD. Our address is 201 West Mission Street San Jose CA 95110. Deputy Chief Shawny Williams, Captain Ed Schroder, Captain Dave Tindall, myself, and several other Lieutenants will be in attendance.

When you arrive, please let the Officer at the front desk know that you are there to see me. I will walk down and bring you upstairs. Should you have to cancel for any reason, please call me at 408-277-4166.

Lt. Paul Joseph #3148
San Jose Police Department
BOI/Robbery

Villarreal, Monique

From: Joseph, Paul
Sent: Tuesday, June 26, 2018 2:48 PM
To: Villarreal, Monique
Subject: Fw: Thanks again for the time.
Attachments: br_faceplus.pdf

From: Todd Pastorini <TPastorini@DATAWORKSPLUS.com>
Sent: Tuesday, April 17, 2018 3:37 PM
To: Joseph, Paul
Subject: Thanks again for the time.

Lt. Joseph,

Thanks again for today. I will be sending you several emails with some information on Facial Recognition. DataWorks Plus is willing to offer a 90 day free evaluation of our Facial Recognition System. DataWorks Plus is the number one provider of Facial Recognition systems on the west coast with installations at:

Los Angeles County Sheriff's Department	9 Million Records
San Bernardino/Riverside County Sheriff's Department	2.7 Million Records
San Diego County Sheriff's Department	2.5 Million Records
Sacramento County Regional	1.75 Million Records
Santa Barbara County Sheriff's Department (pending install)	1 Million Records
San Francisco Police Department	1 Million Records

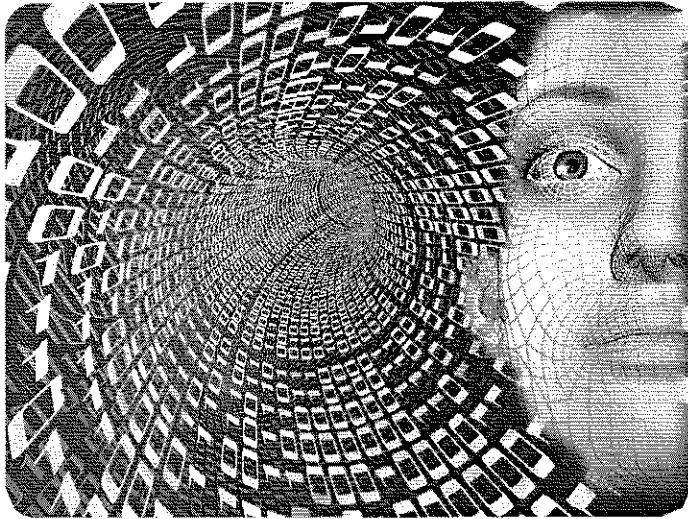
The system is capable of real time searching by any user on the system by either workstation or Mobile device, such as the evolution. We are partnered with NEC, Rank One, and Cognitec to be able to offer you the best matching engine to meet your budget. I am working on the updated proposals and will get those to you when they are done.

Sincerely,
Todd Pastorini
Executive Vice President & General Manager
DataWorks Plus
(925)240-9010

• Mugshot Management • LiveScan Plus™ • Digital CrimeScene™ • Mobile Identification • Facial Recognition • Video Management

FACEPlus

*Accurate, Reliable
Identification with the
Latest Facial Recognition Technology.*



Generates facial templates from mugshots or any facial image repository

User-customized image display for investigations

Search millions of images in seconds

Searches facial features and ignores features such as hair color, eyeglasses, and background

Image editing tools for improved matching

Video and photo input support

Pose Correction that allows the use of off-angle images such as surveillance

Case Management

Track and store multiple search scenarios in a case. You can input and manage multiple views of probe images taken from JPEG or TIFF single image files as well as AVI and MPEG video files. Then you will be able to create a variety of searches with different probe images and data field selections for filtering. Each search will be saved in the case file. Select a combination of searches to review a blended result based on match scores.

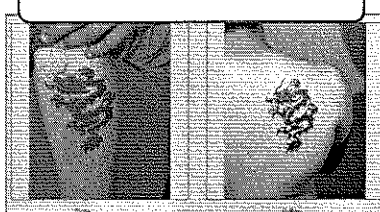
Image Enhancement

Images can be edited to provide even more accurate results by marking the eye locations, cropping the images to be similar, correcting image brightness, and other basic editing functions. Pose correction and lighting normalization is also available, allowing you to search facial images that were once unsearchable.

Facial Comparison

Compare images side-by-side or edit copies of images for easier viewing or to clarify certain details. You can overlay two images to view distinct images, or view a "curtain" image, which displays the left portion of one image and the right portion of the other image.

Tattoo Matching

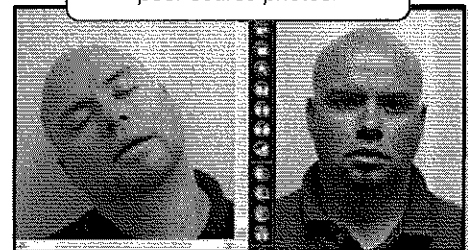


MATCH



Create and manipulate 3D models to the view you need.

Select eye locations and match poor source photos.



MATCH

DataWorks Plus

Accurate, Reliable Identification

From a Leader in Law Enforcement & Criminal Justice Technology



FACE Plus uses the latest in facial recognition technology.

FACE Plus conducts a one-to-many search of your entire database and will display photos and data when matches are found.

- ◆ Investigations
- ◆ Intake identification
- ◆ Movement identification
- ◆ Release identification
- ◆ Watch list comparison
- ◆ Mobile Data Terminal (MDT)



See What Our Customers have to say about DataWorks Plus...

"Awesome company to deal with, very flexible and always quick to respond to my concerns. It really makes me feel like a partner in the process, not just a client."

"DataWorks stood by every promise made during the pre-sale meetings. There were no "bait and switch" tricks or false representations made. They delivered a great product, on time, and the customer service has been excellent."

Applications

Images can be checked at intake, release, or movement as well as on a mobile data terminal for inmate verification. FACE Plus can even be used to perform a comparison against your Watch List database to identify wanted individuals.

Investigations

Images can be uploaded to conduct a one-to-many facial recognition search. FACE Plus gives the user the option to narrow the search by physical characteristics. All matches to the facial recognition search will be displayed by photo, which allows you to view each record with additional photos and data for further identify verification.

Watch List

FACE Plus can ensure all records are screened against your user defined watch list or other database for wanted individuals. The watch list monitor gives real-time feedback if a hit occurs against the watch list. You can view all matches and associated images. Contact information and protocols displayed with the match make it easy for the right procedures to be followed if a match occurs.

Identification at Booking

Inmates can be screened at booking to verify if they have a previous record. If a facial recognition hit is returned, you can choose to automatically import the existing data from the previous booking into the new booking.

DataWorks Plus

728 North Pleasantburg Drive
Greenville, SC 29607
Phone: 866-632-2780
Fax: 864-672-2787
E-mail: sales@dataworksplus.com

www.dataworksplus.com